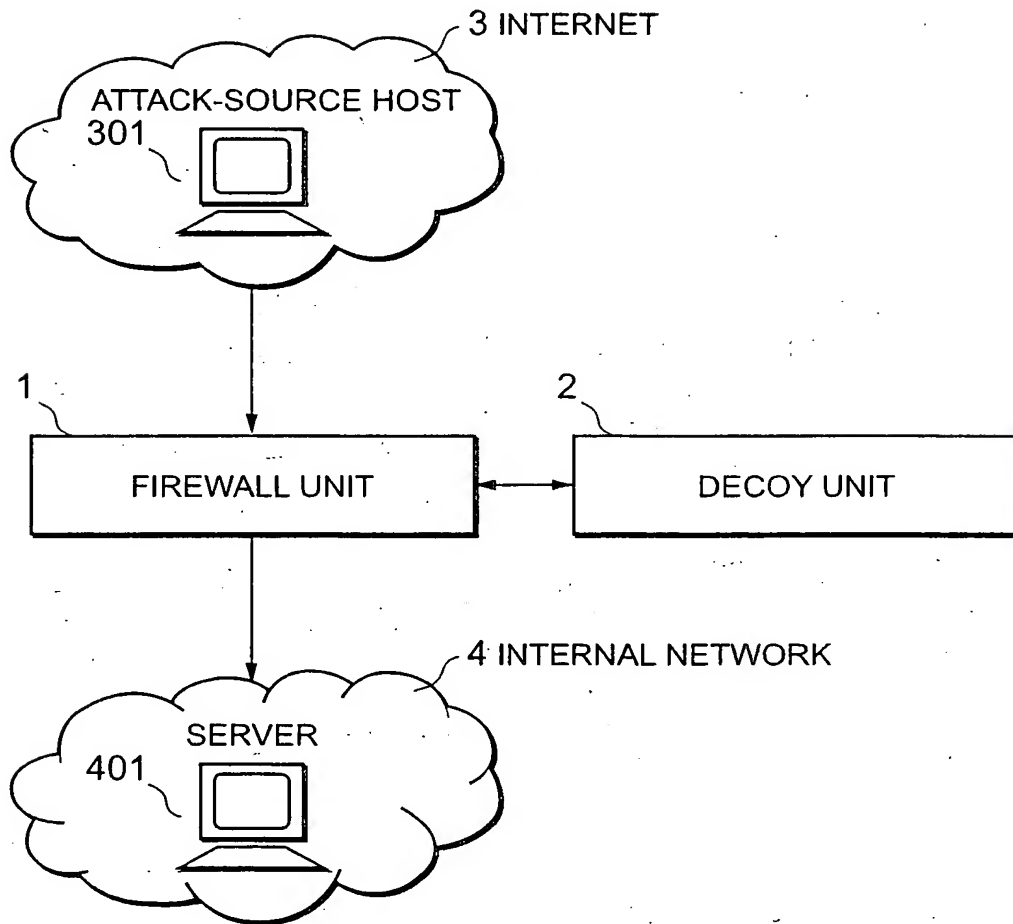


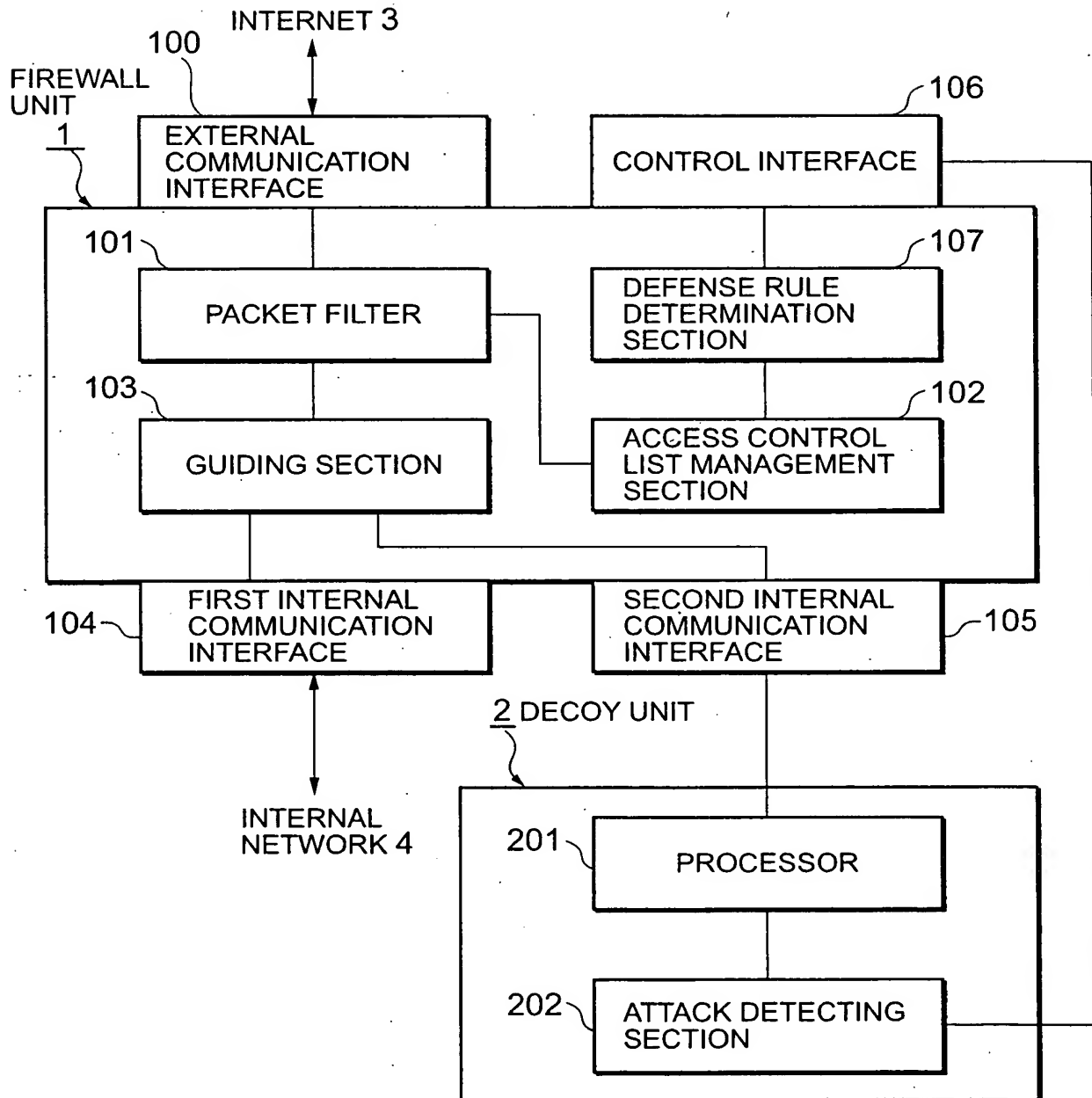


FIG. 1



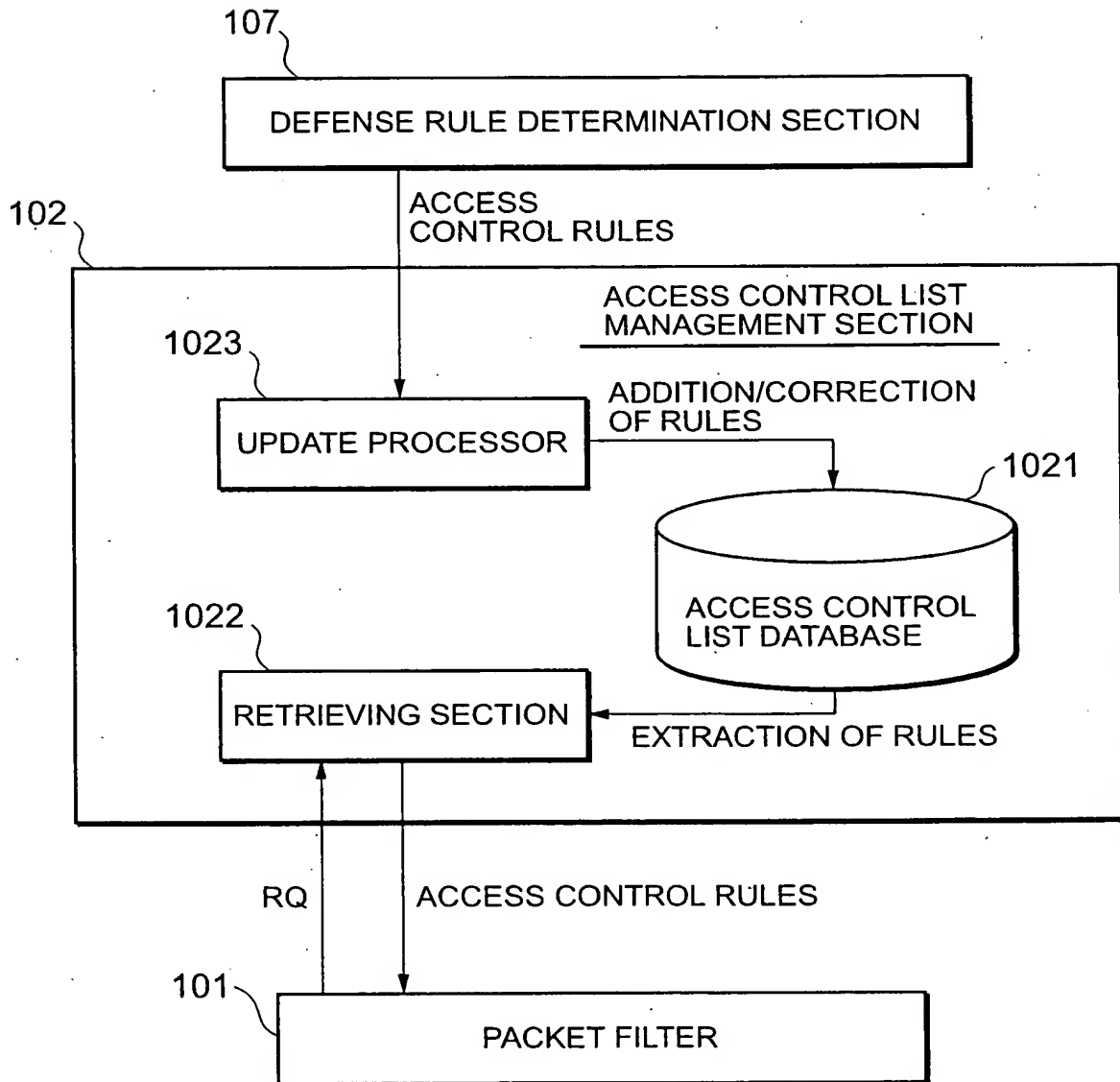
2/55

FIG. 2



3/55

FIG. 3



4/55

FIG. 4

1021

ACCESS CONTROL LIST DATABASE		
SOURCE IP ADDRESS (SRC)	DESTINATION IP ADDRESS (DST)	PACKET FILTERING PROCESS (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

\* : MATCHED WITH ARBITRARY ADDRESS

ACCEPT : ACCEPTANCE OF PACKET

DENY : DENIAL OF PACKET (WITH ICMP ERROR NOTIFICATION)

DROP : DROPPING OF PACKET (WITHOUT ICMP ERROR NOTIFICATION)

FIG. 5

## GUIDING LIST

1.2.3.1
1.2.3.2
1.2.3.3
1.2.3.5
1.2.3.6
⋮

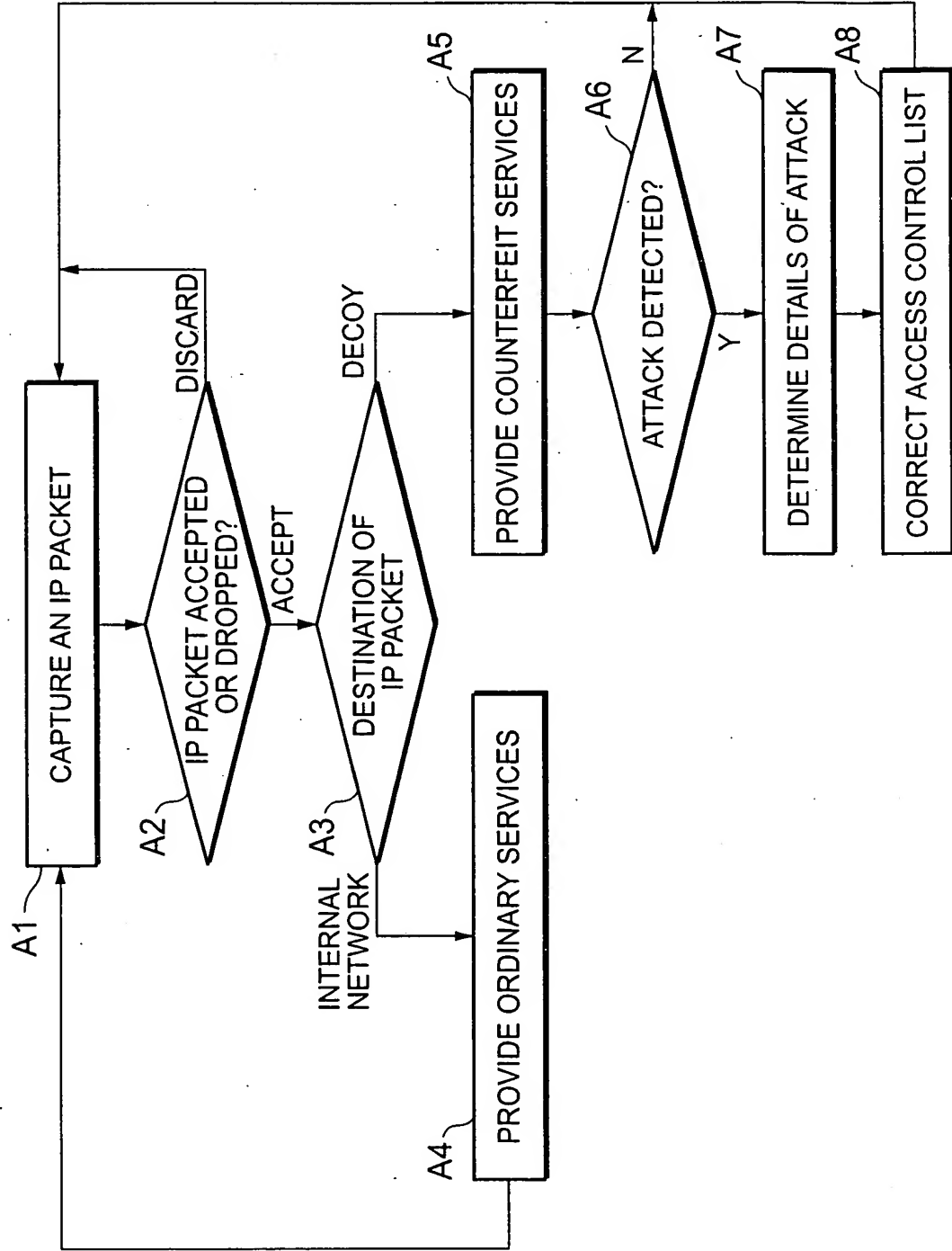
FIG. 6

107

DEFENSE RULE DETERMINATION SECTION			
ATTACK TYPE	SOURCE IP ADDRESS (SRC)	DESTINATION IP ADDRESS (DST)	PACKET FILTERING PROCESS (PROC)
RECON	—	—	—
INTRUSION	\${SRC_IP_ADDRESS}	*	DROP
DESTRUCTION	\${SRC_IP_ADDRESS}	*	DROP

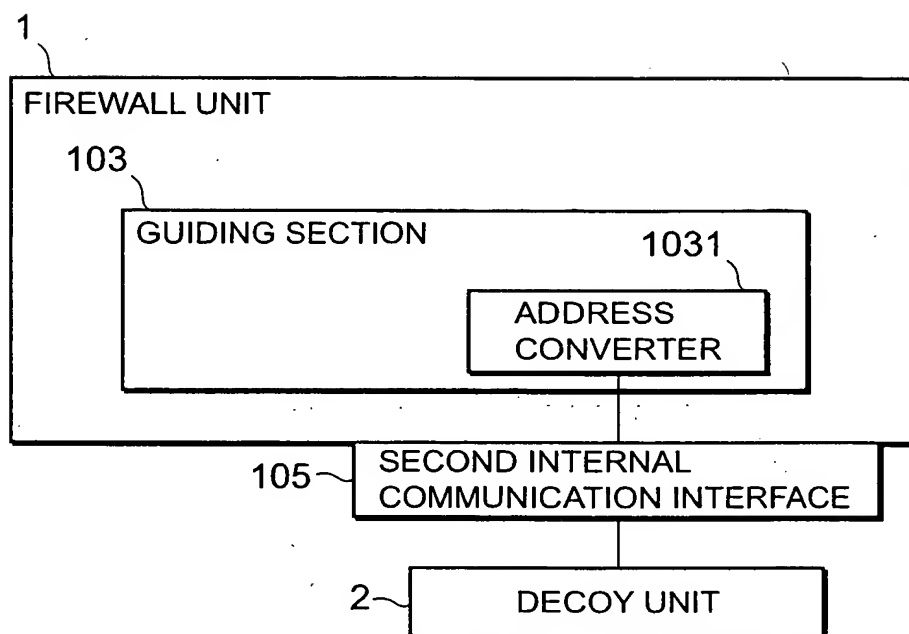
- : WITHOUT ANY ADDRESS (NO PROCESSING)  
 \${} : VARIABLE TO BE REPLACED

FIG. 7



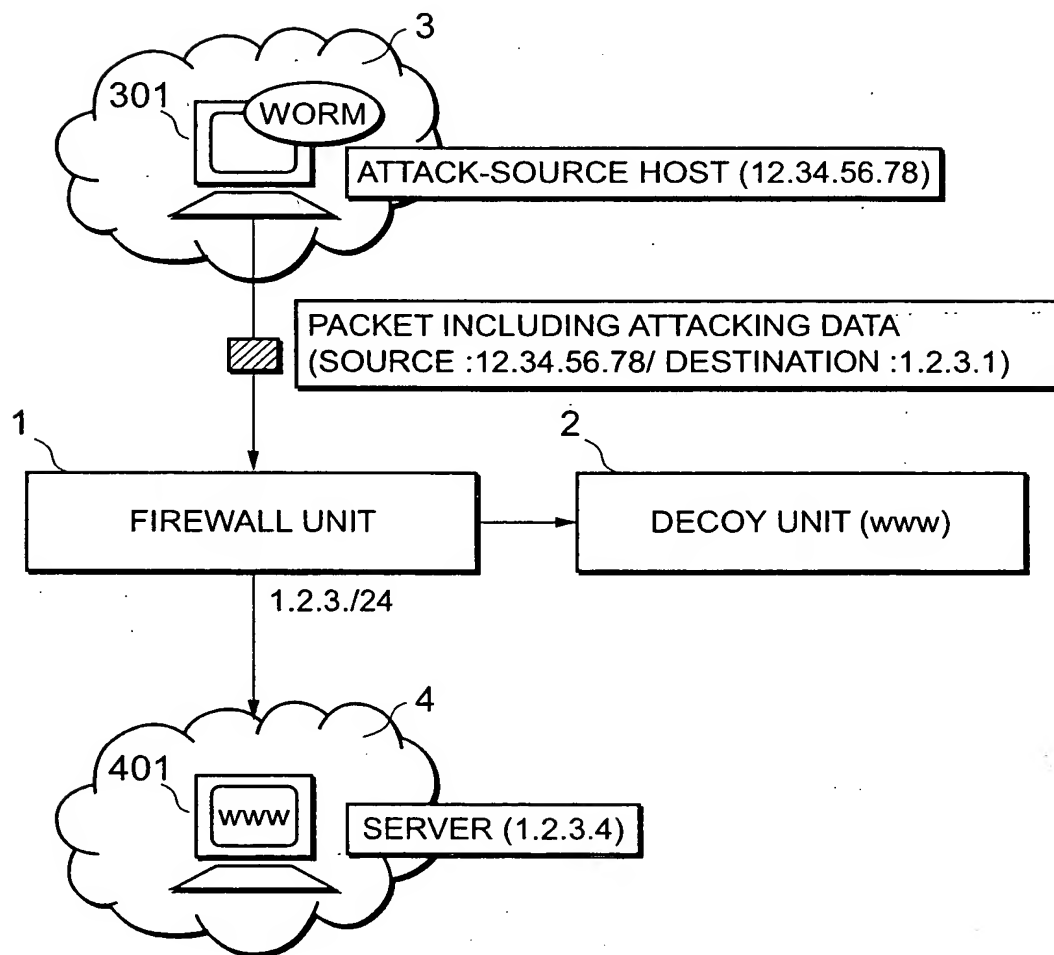
7/55

FIG. 8



8/55

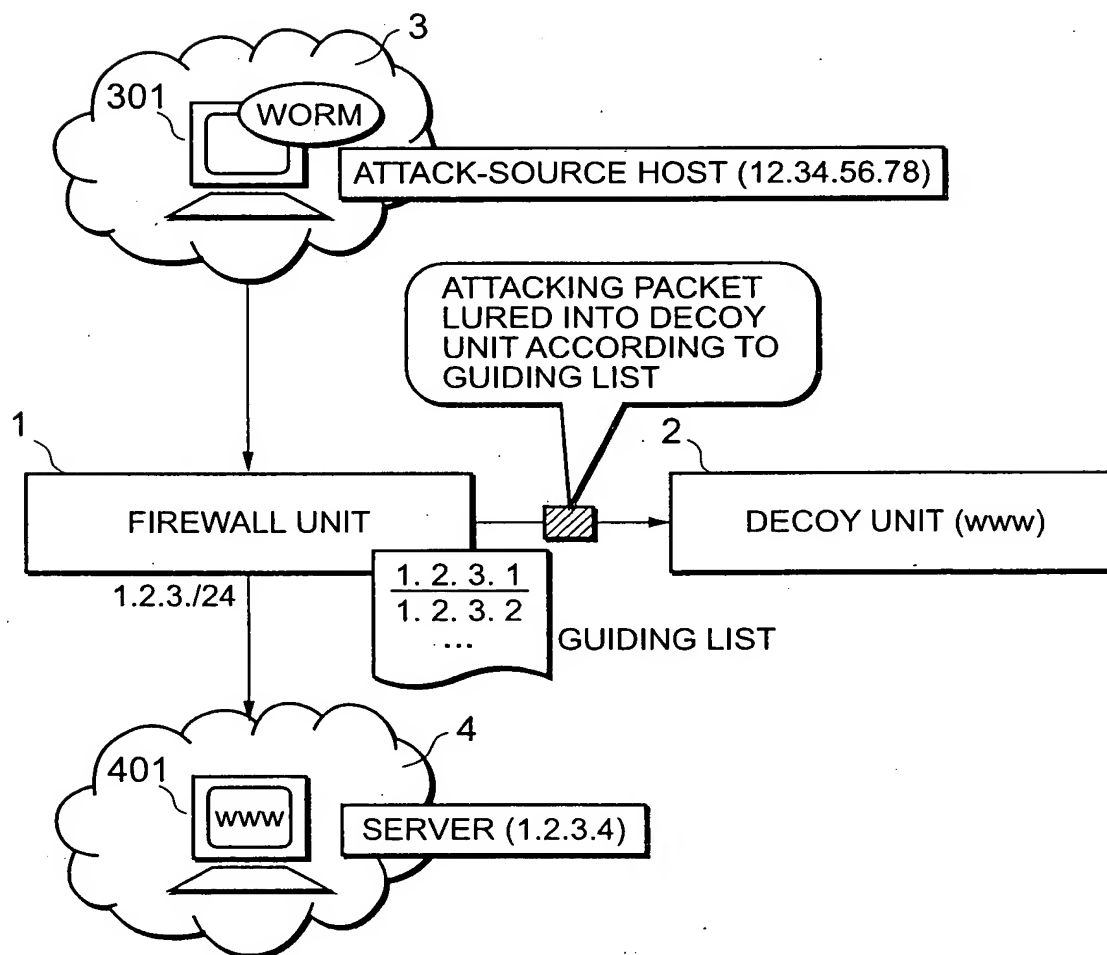
FIG. 9





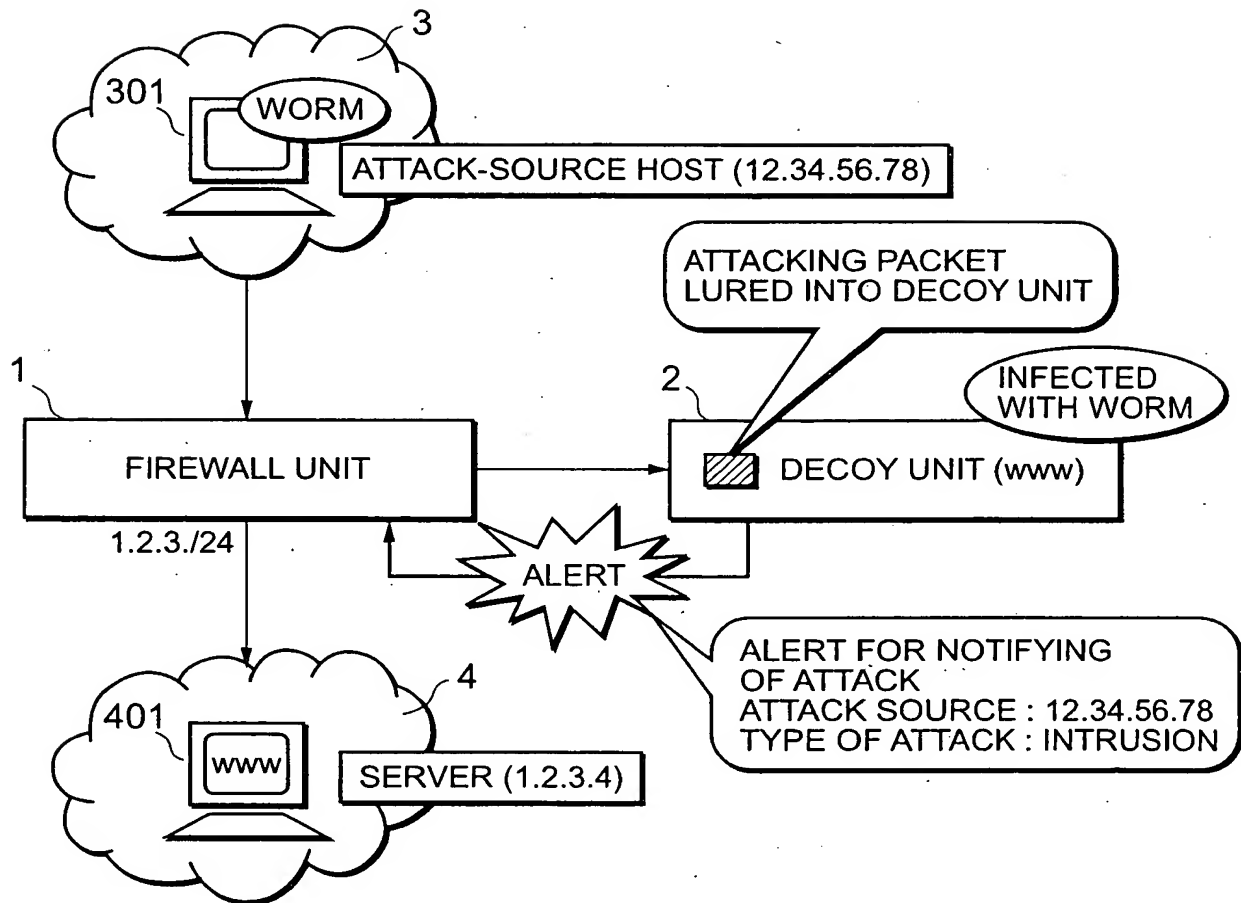
9/55

FIG. 10



10/55

FIG. 11



11/55

FIG. 12

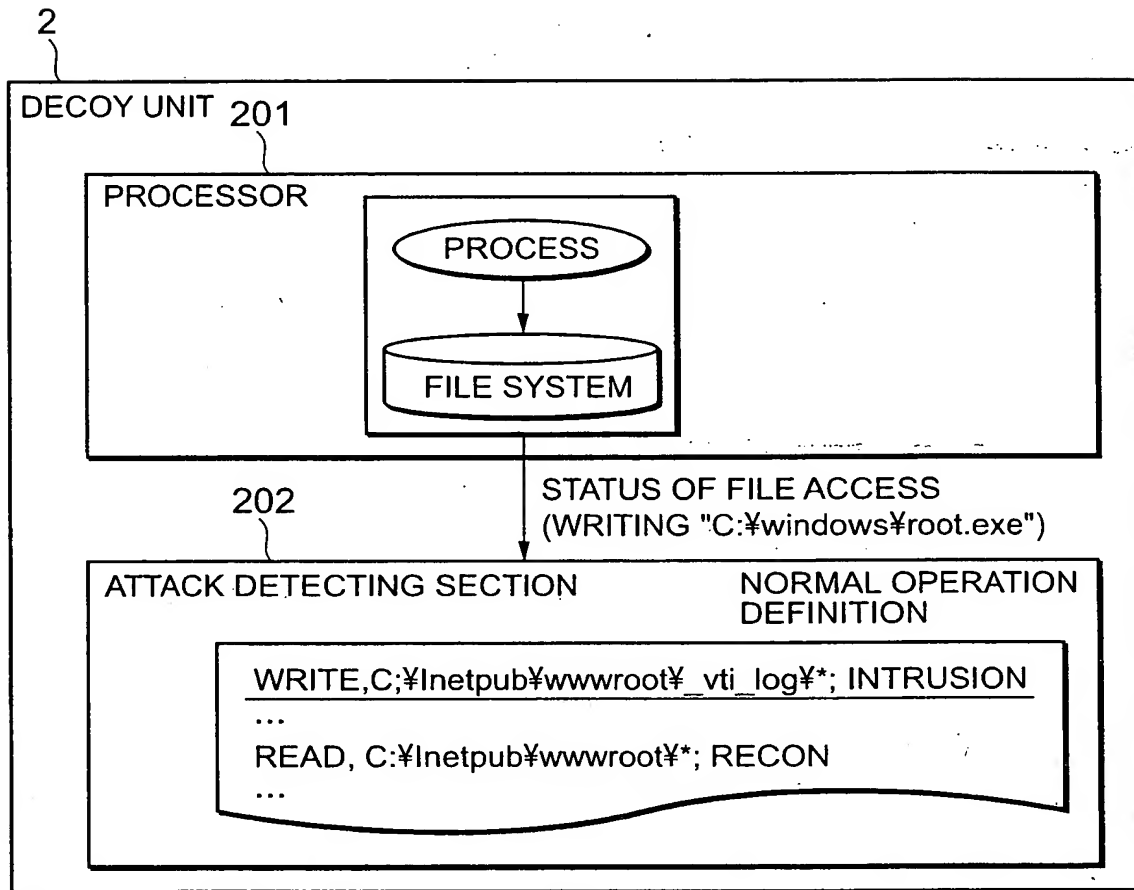


FIG. 13

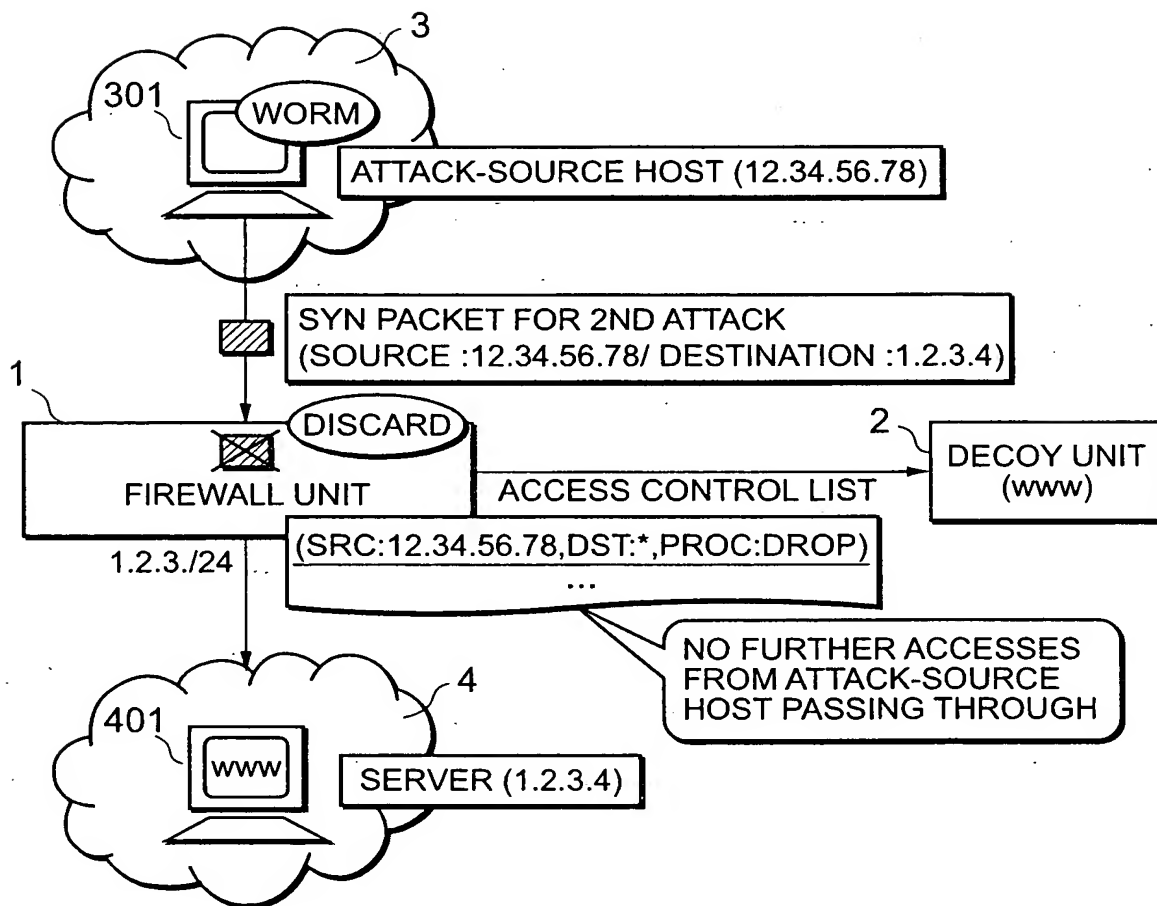
UPDATE OF ACCESS CONTROL LIST

SOURCE IP ADDRESS (SRC)	DESTINATION IP ADDRESS (DST)	PACKET FILTERING PROCESS (PROC)
12.34.56.78	*	DROP
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

ADDITION 

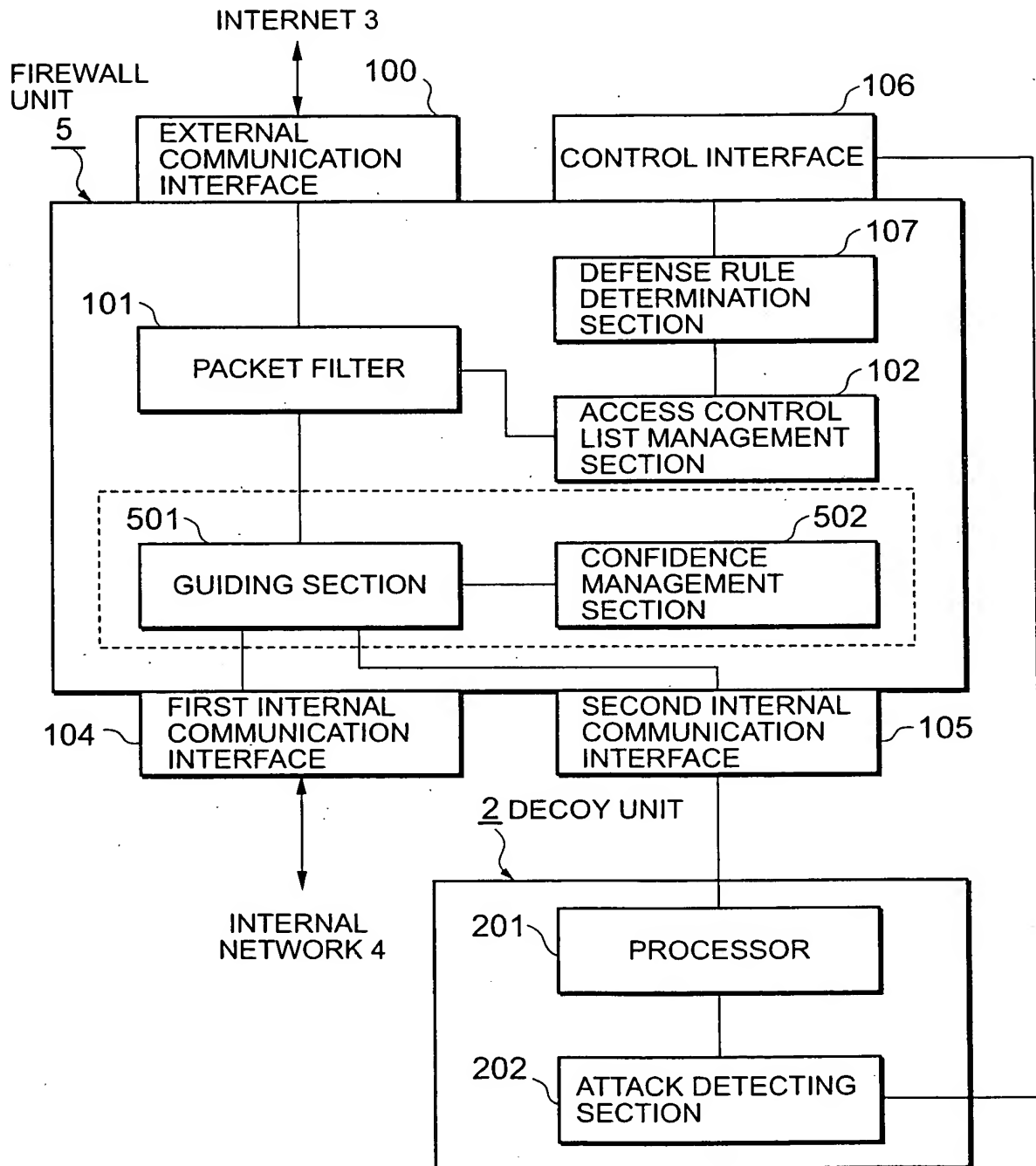
13/55

FIG. 14



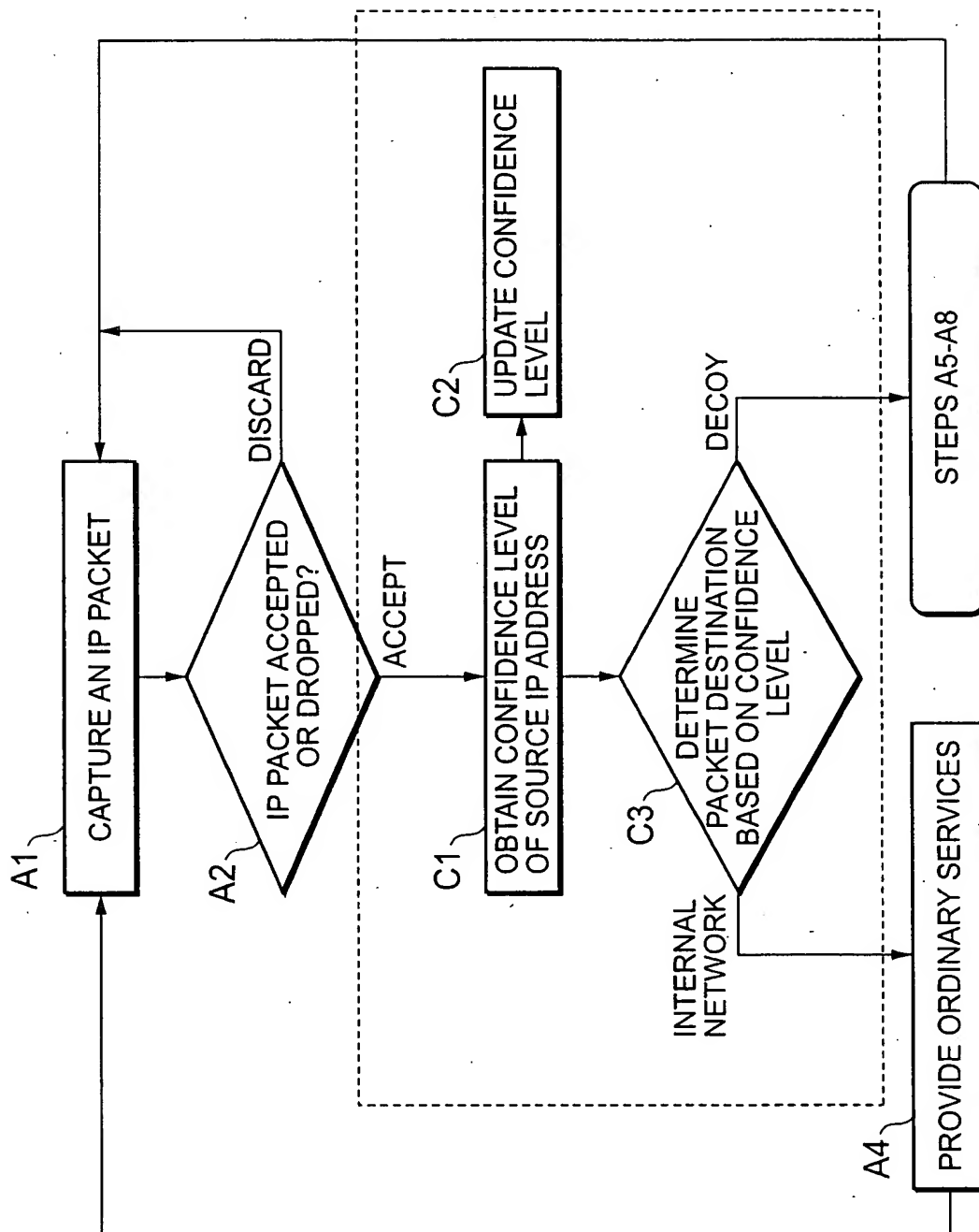
14/55

FIG. 15



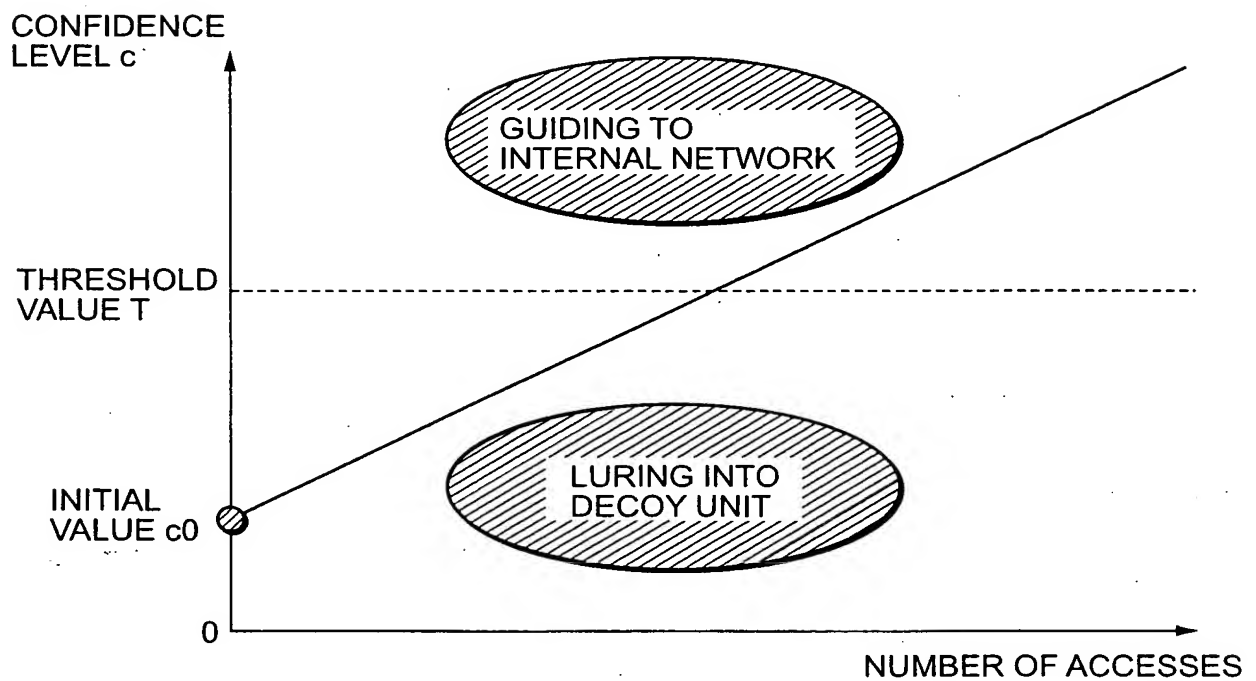
15/55

FIG. 16



16/55

FIG. 17





17/55

FIG. 18A

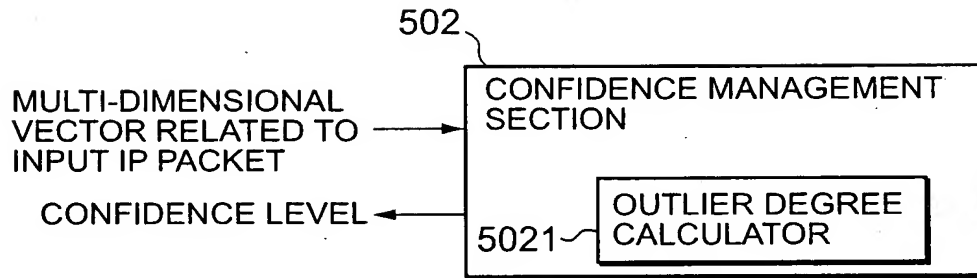
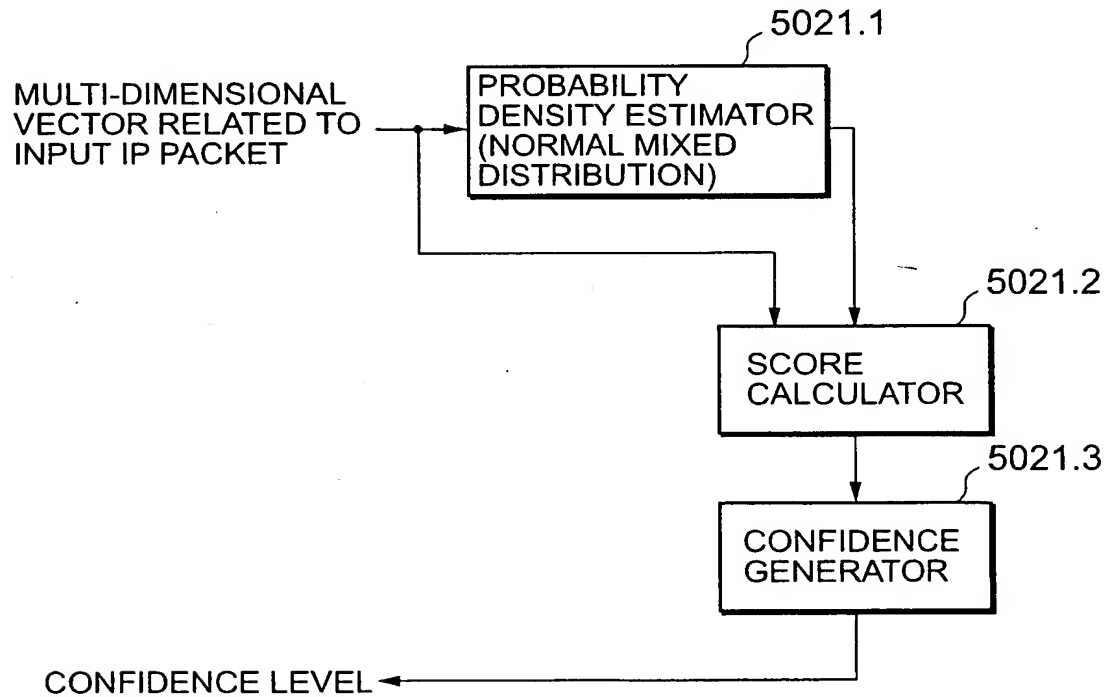
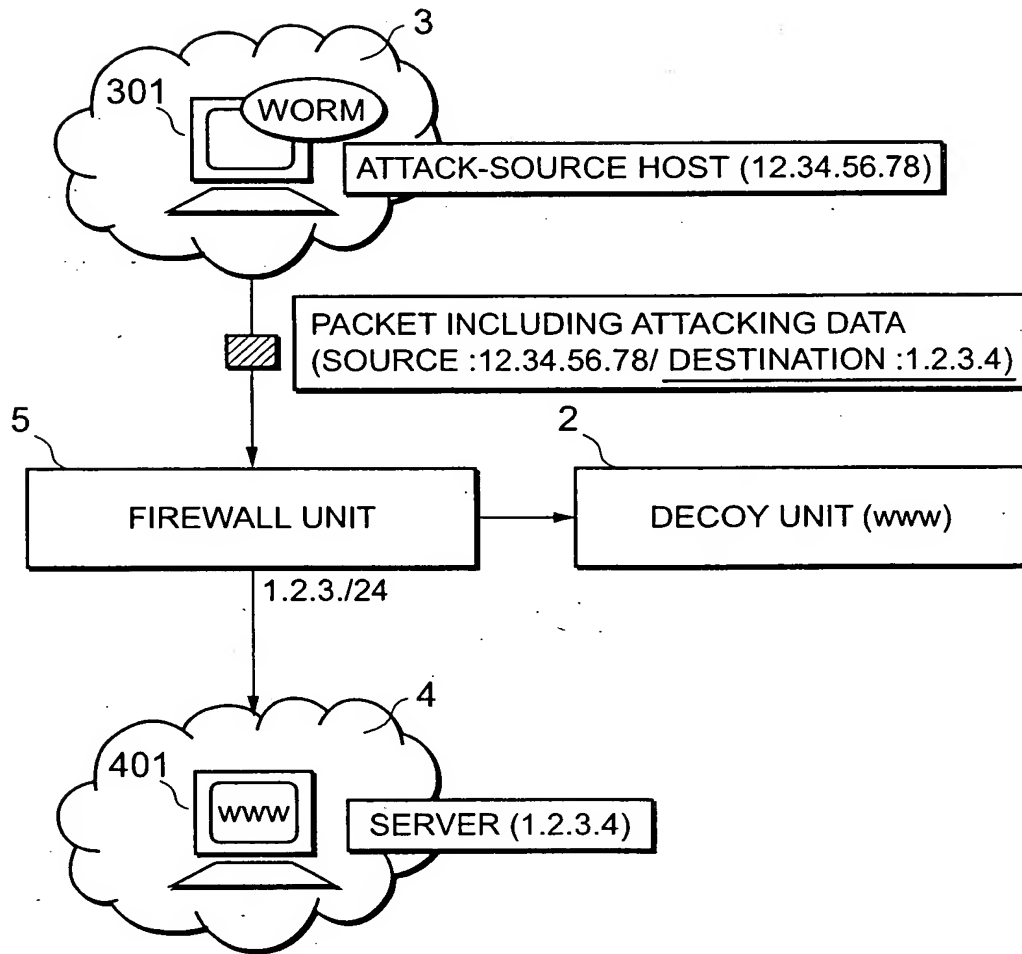


FIG. 18B



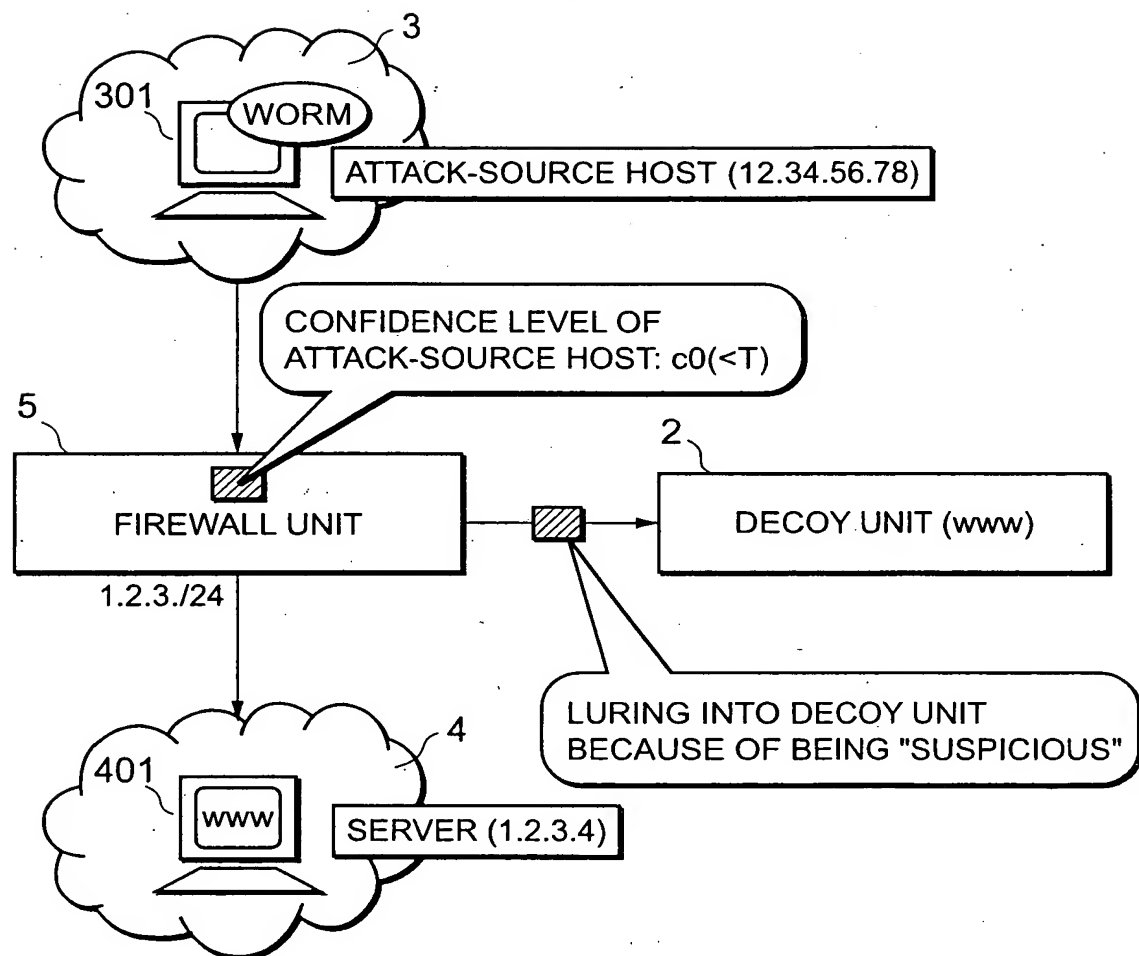
18/55

FIG. 19



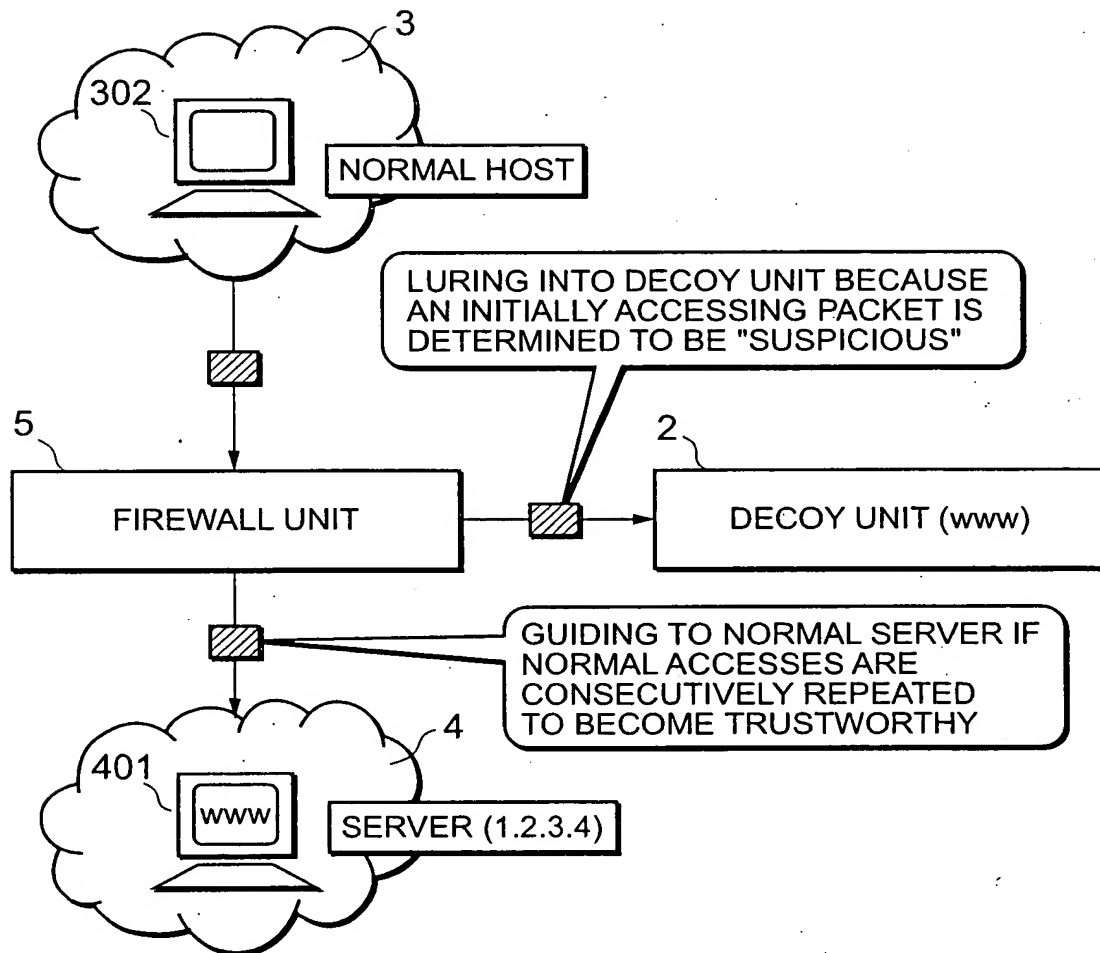
19/55

FIG. 20



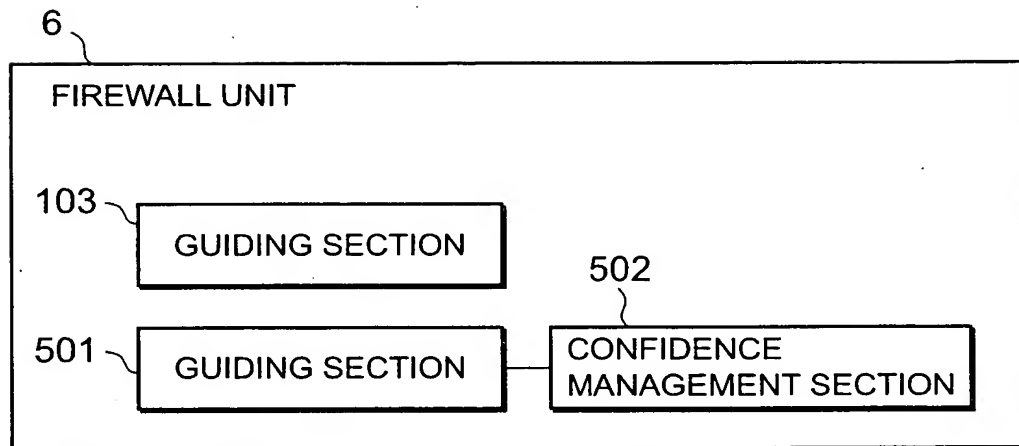
20/55

FIG. 21



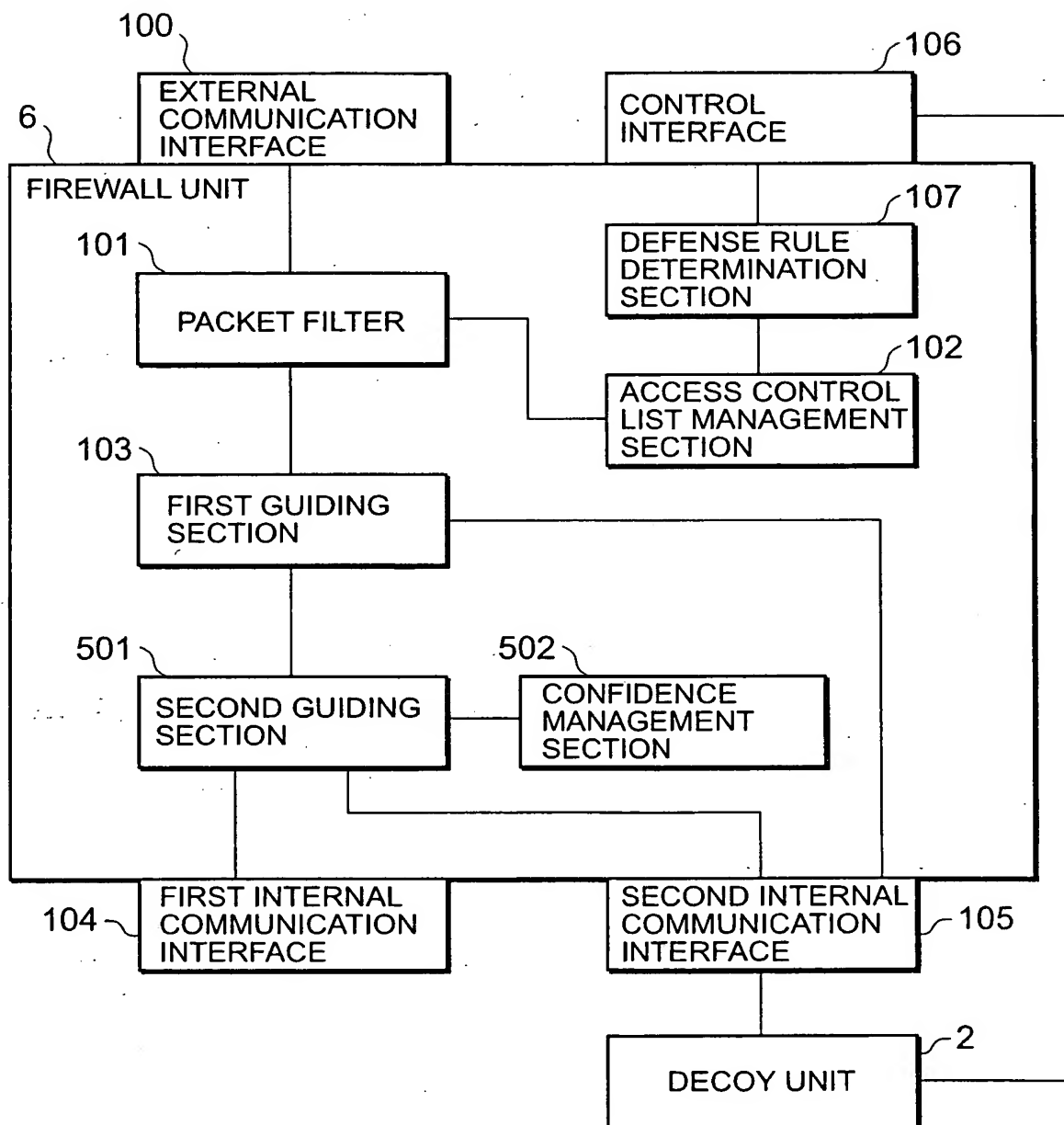
21/55

FIG. 22



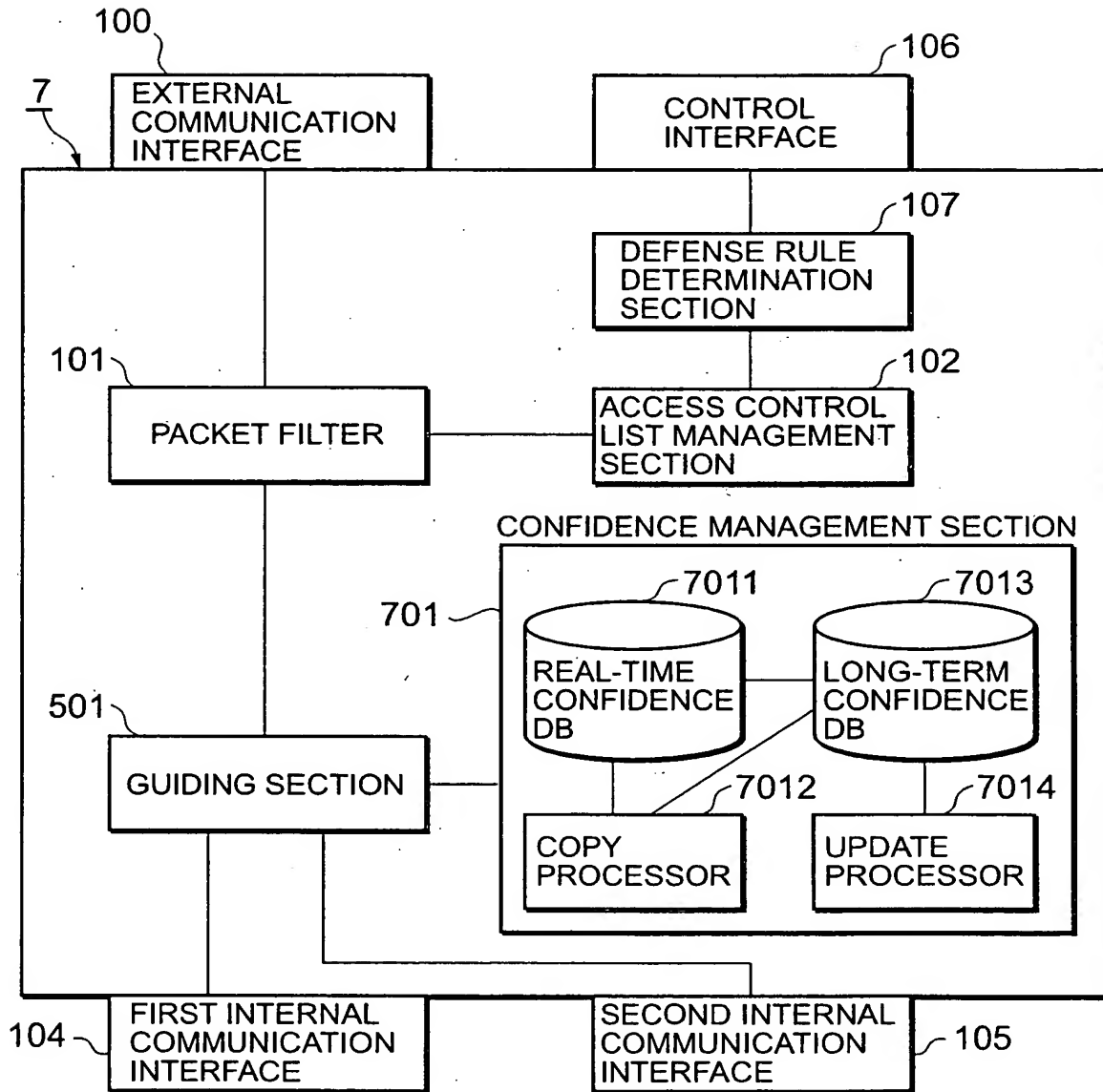
22/55

FIG. 23



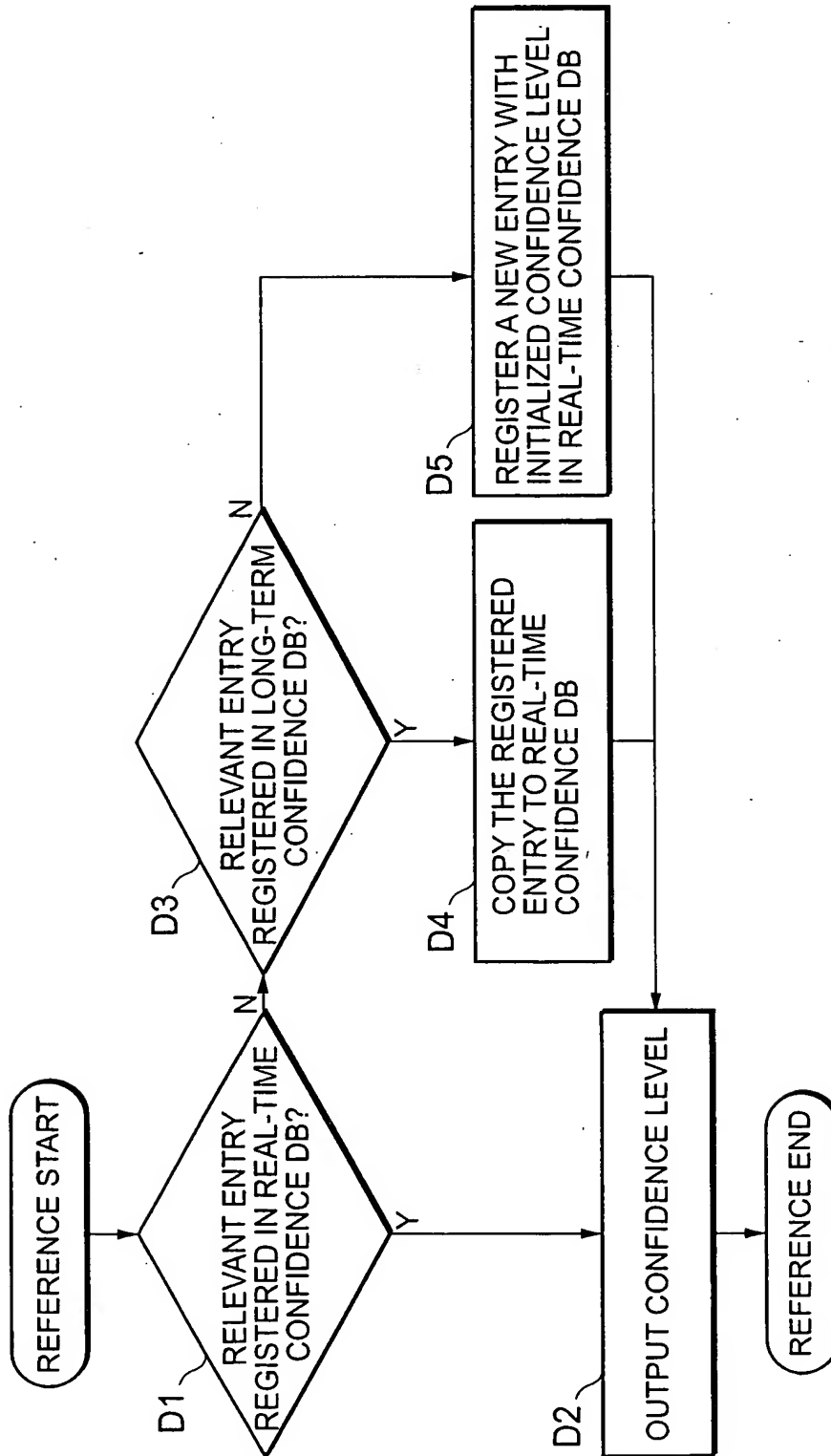
23/55

FIG. 24



24/55

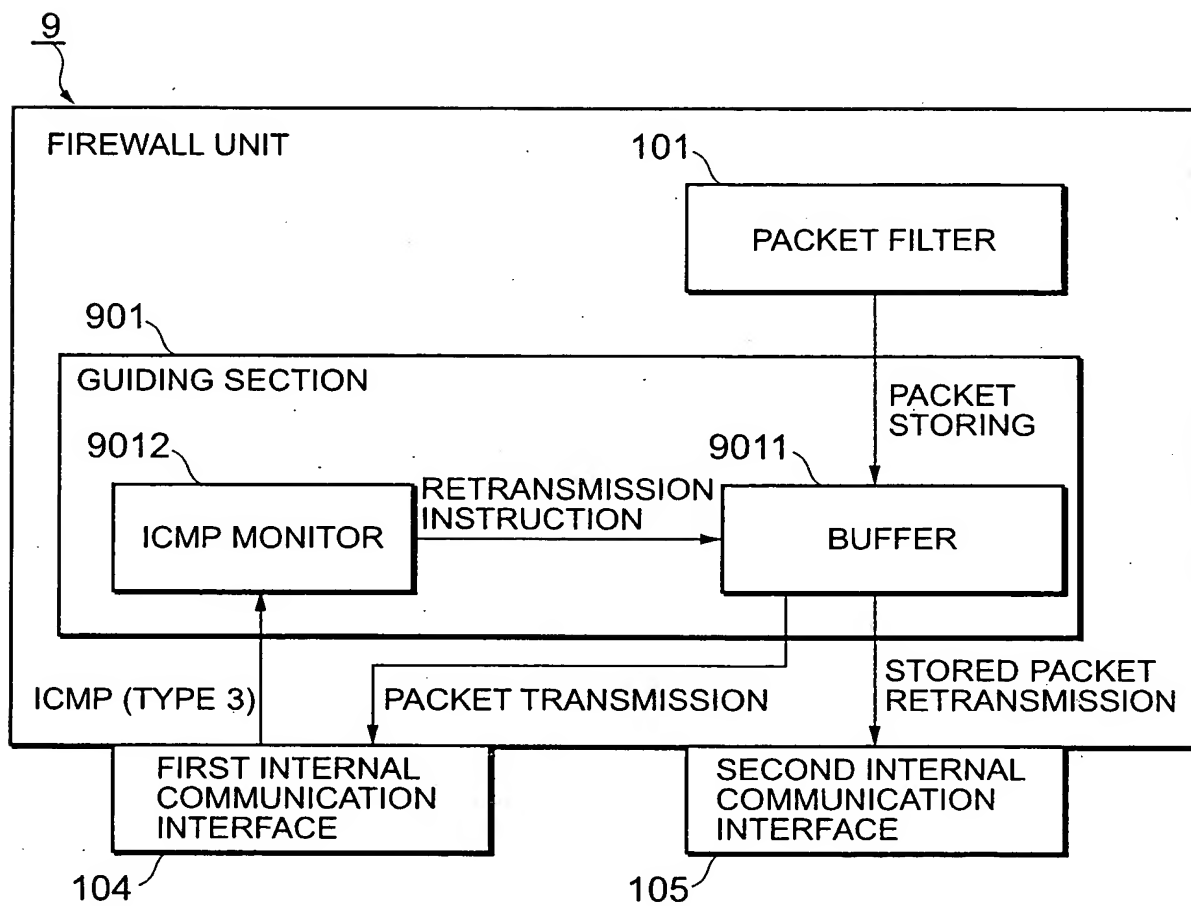
FIG. 25





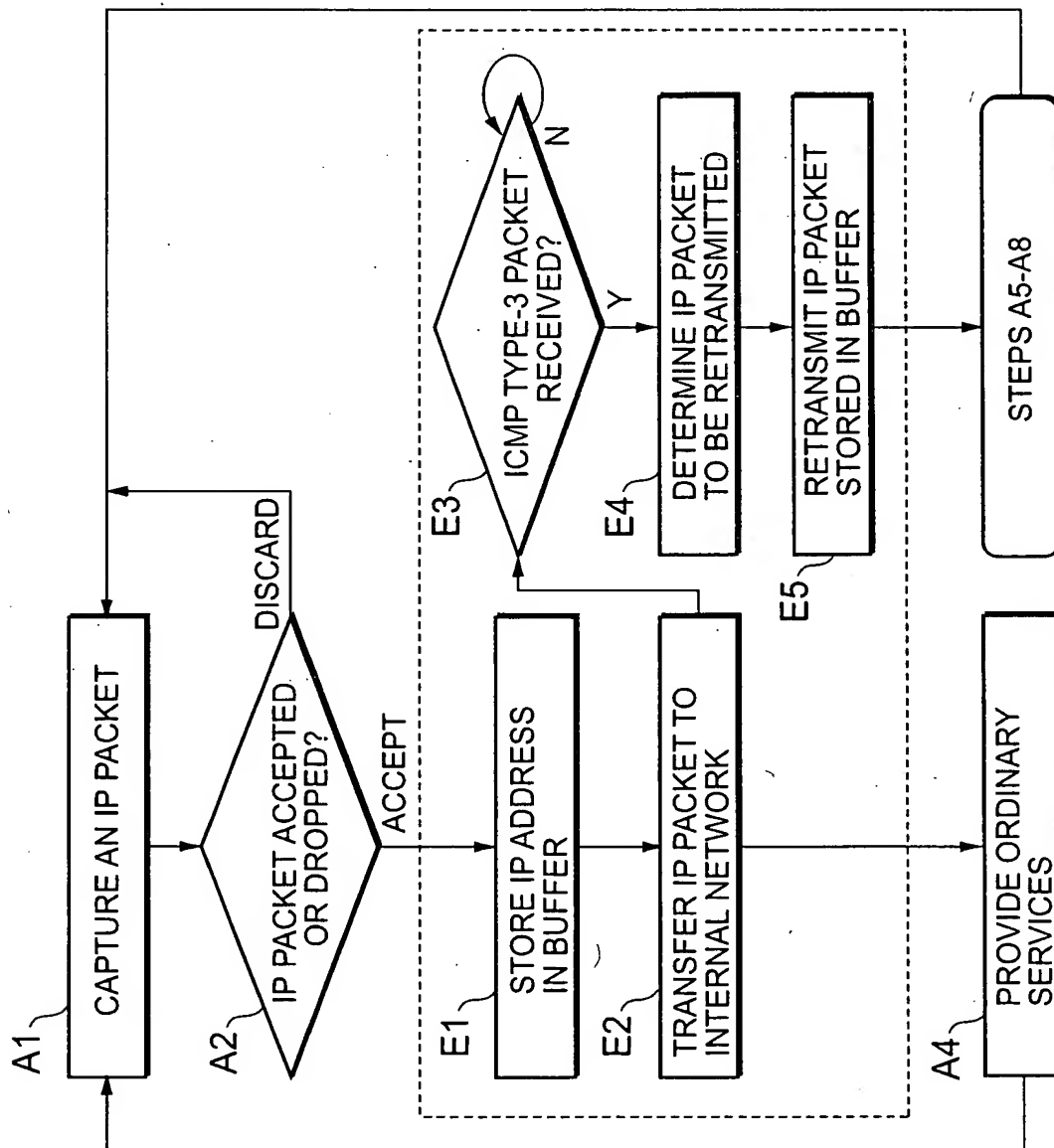
25/55

FIG. 26



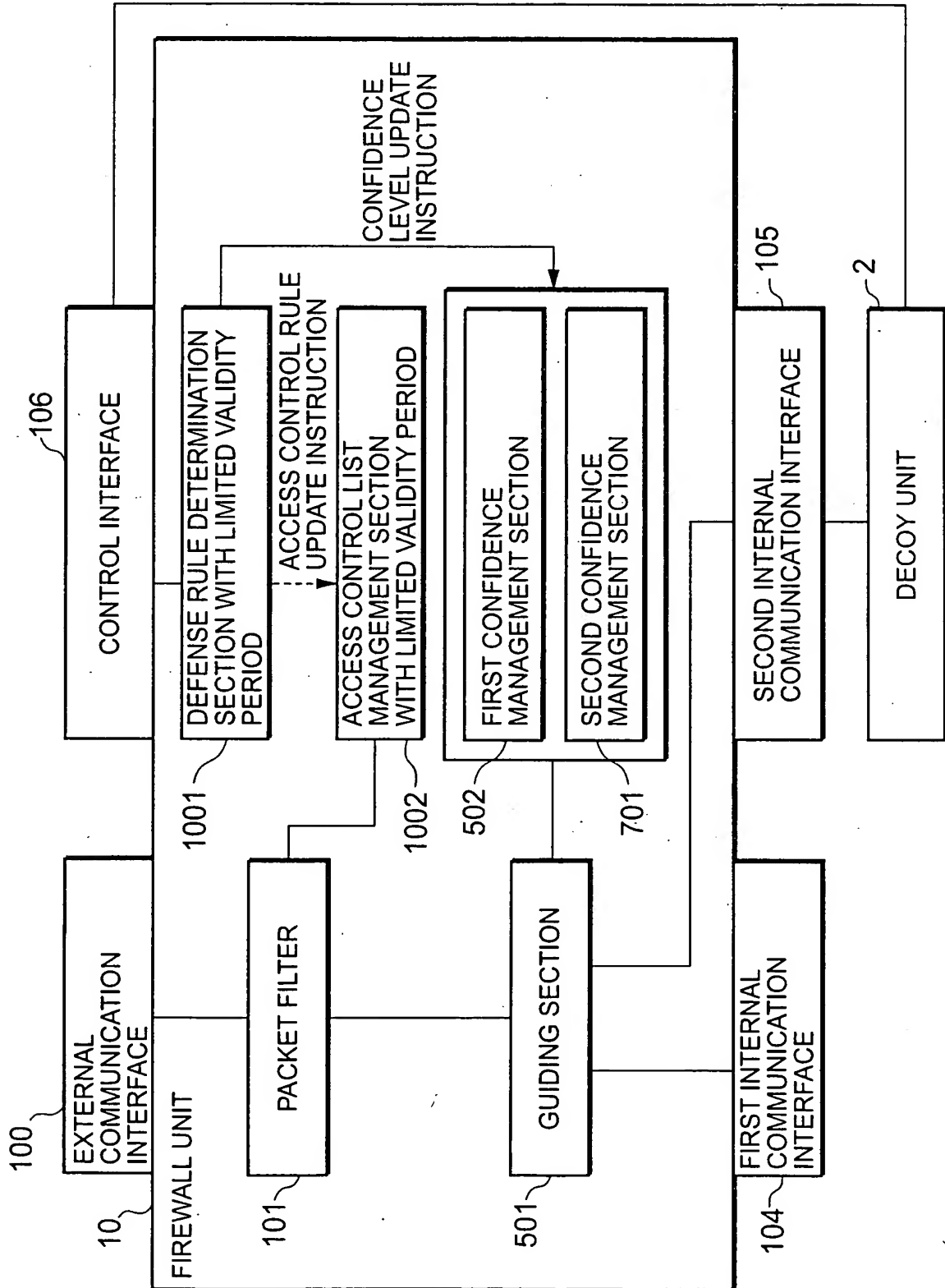
26/55

FIG. 27



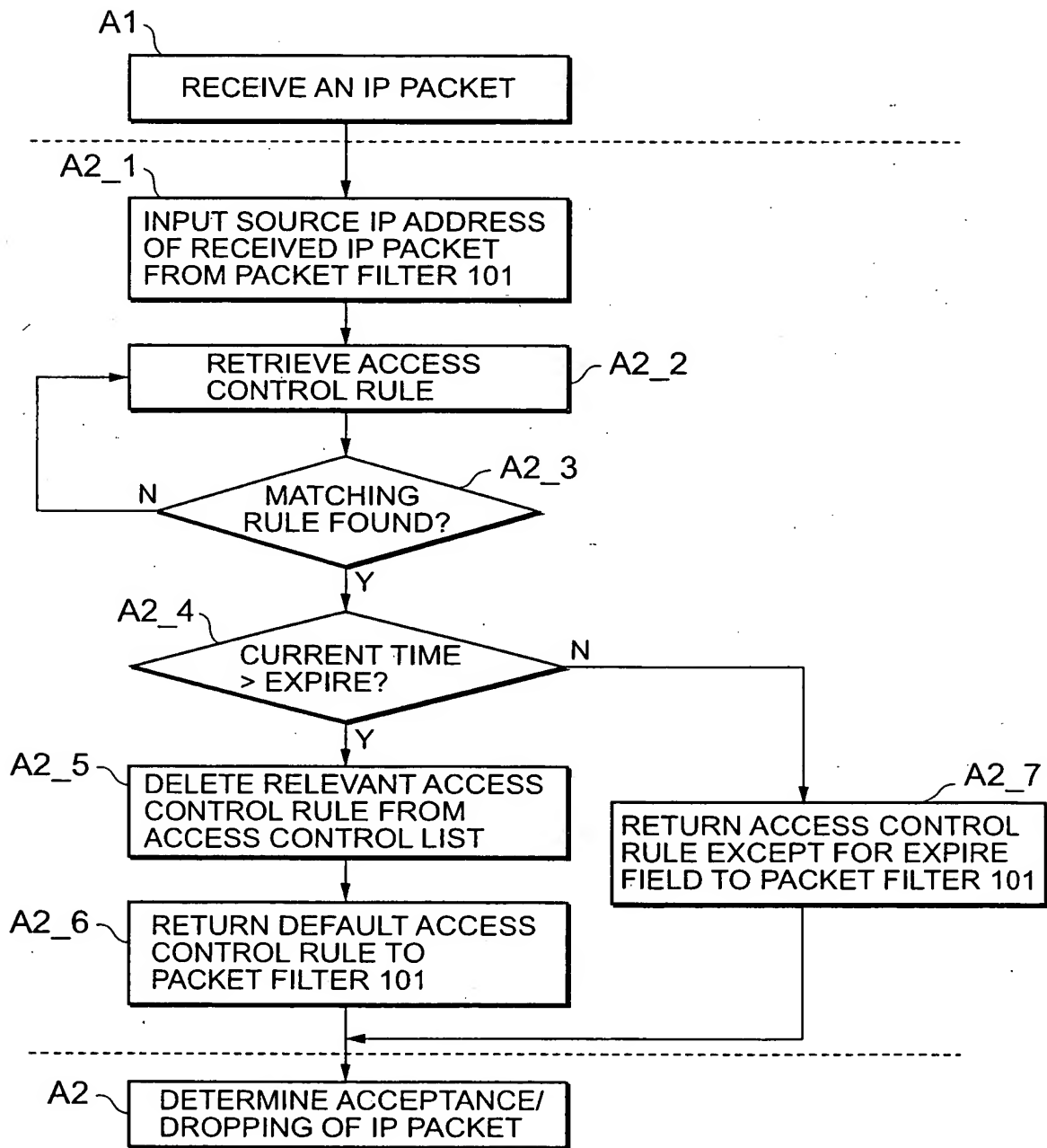
27/55

FIG. 28



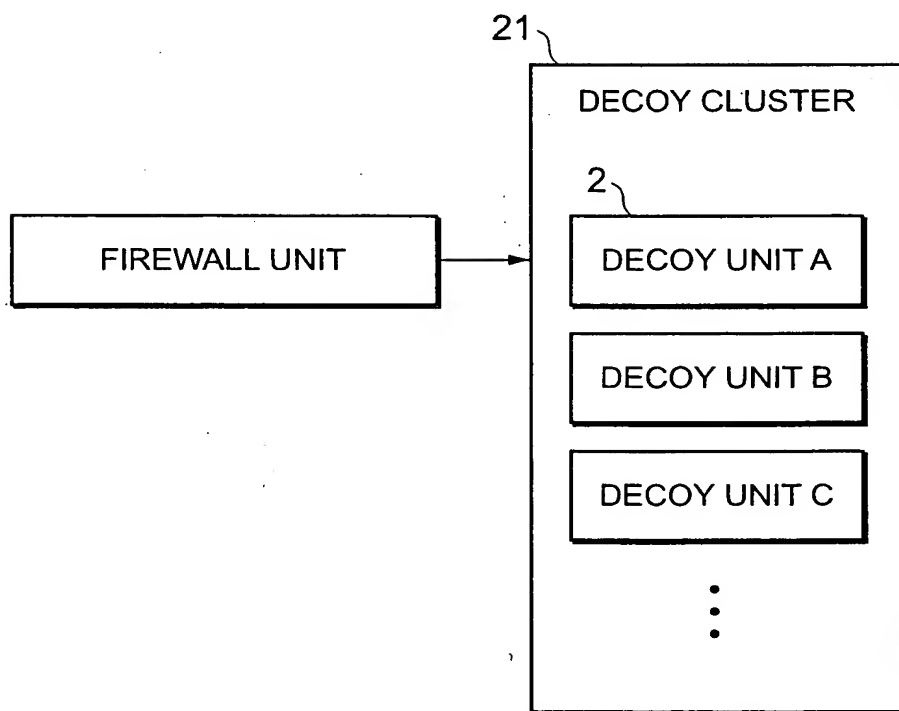
28/55

FIG. 29



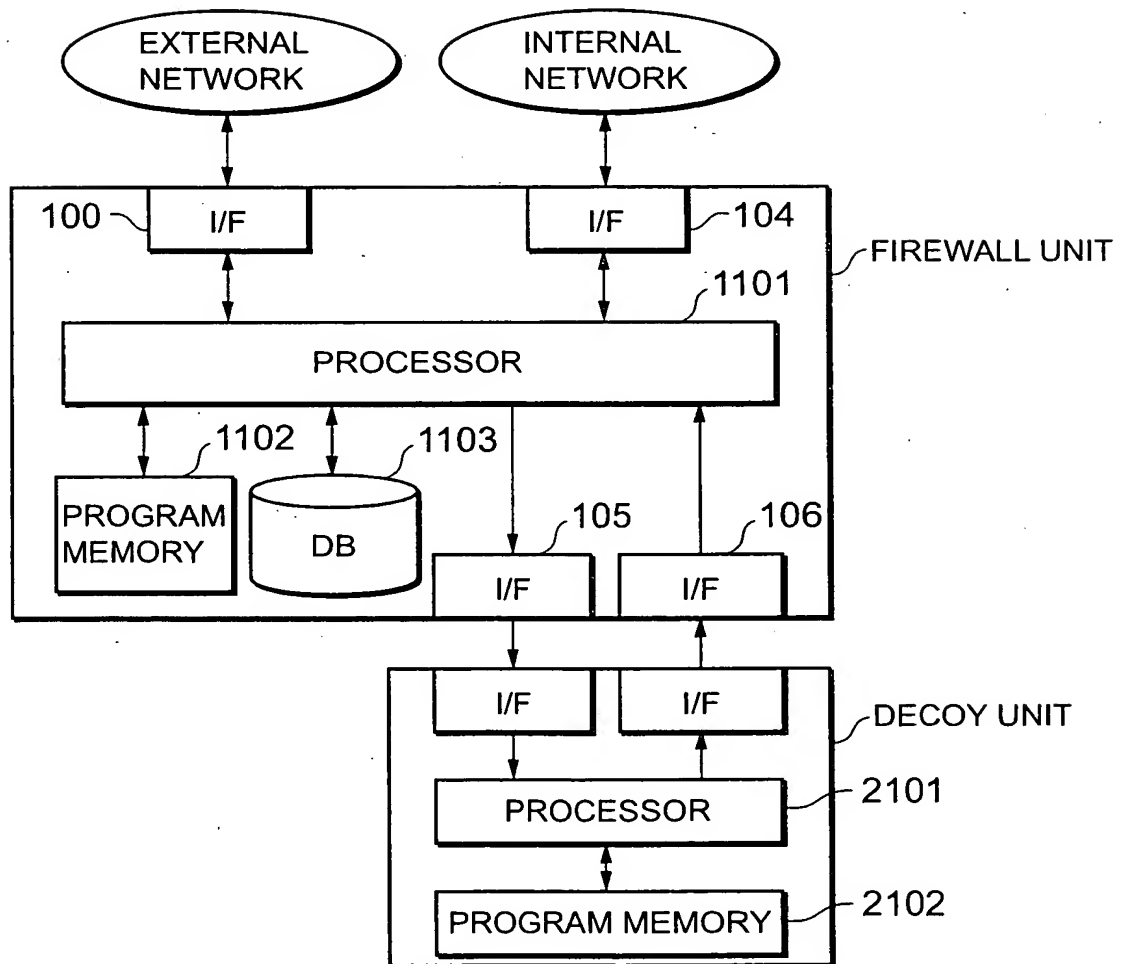
29/55

FIG. 30



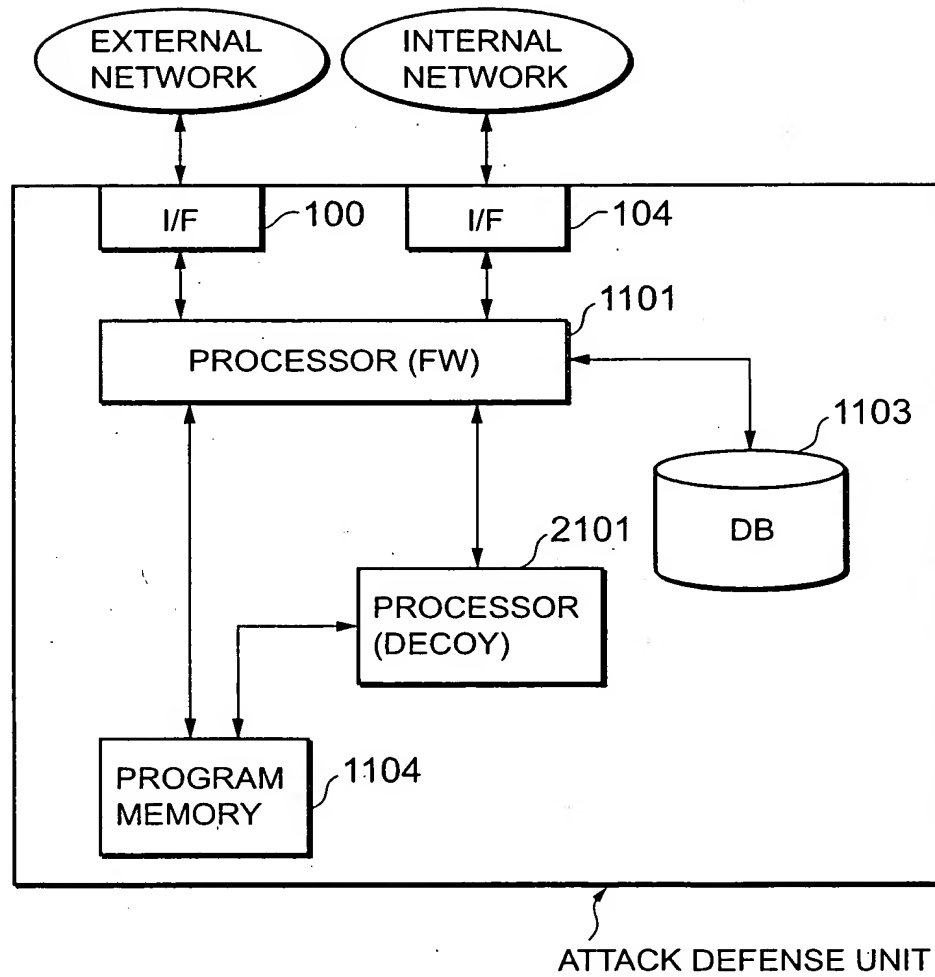
30/55

FIG. 31



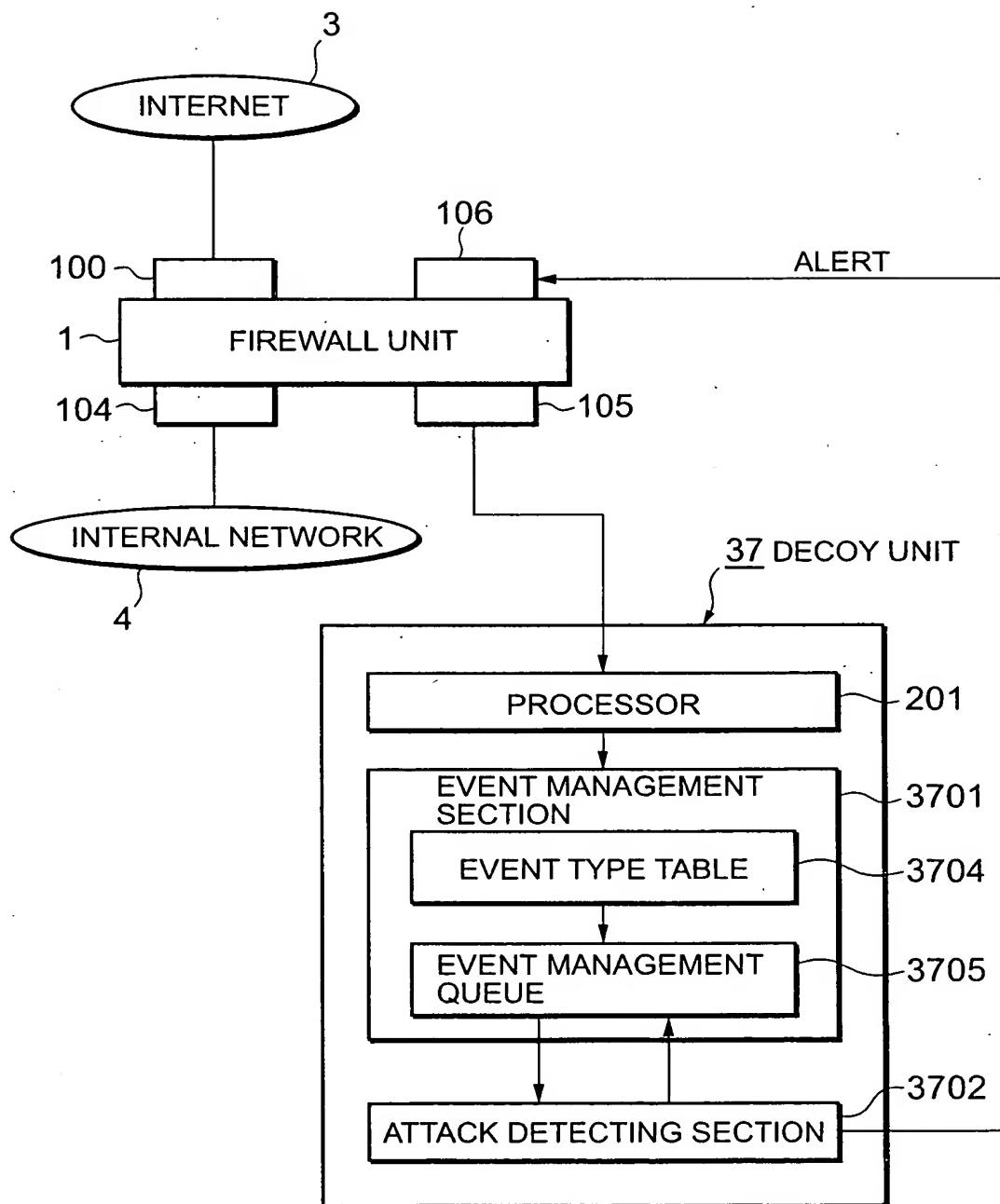
31/55

FIG. 32



32/55

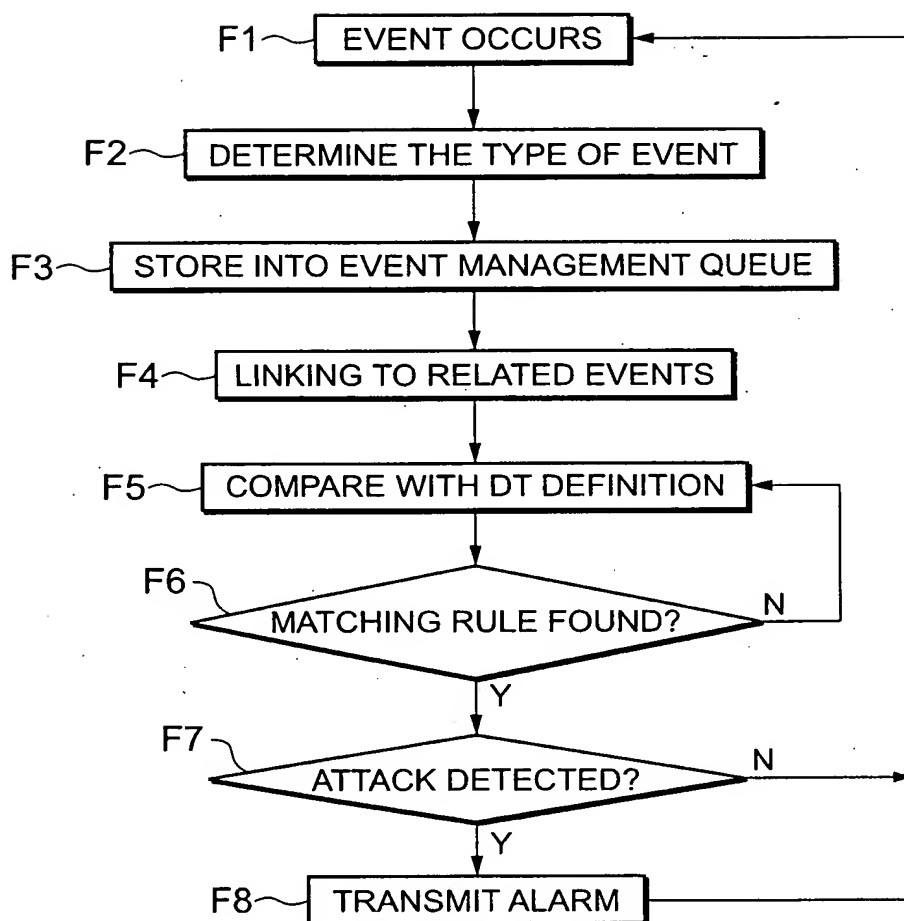
FIG. 33





33/55

FIG. 34



EVENT NAME	EVENT TYPE
PROC_EXEC	PROCESS
PROC_FORK	PROCESS
NW_ACCEPT	NETWORK
FILE_OPEN	FILE

FIG. 36

"NETWORK" EVENT MANAGEMENT QUEUE 

--	--	--	--	--	--	--

"PROCESS" EVENT MANAGEMENT QUEUE 

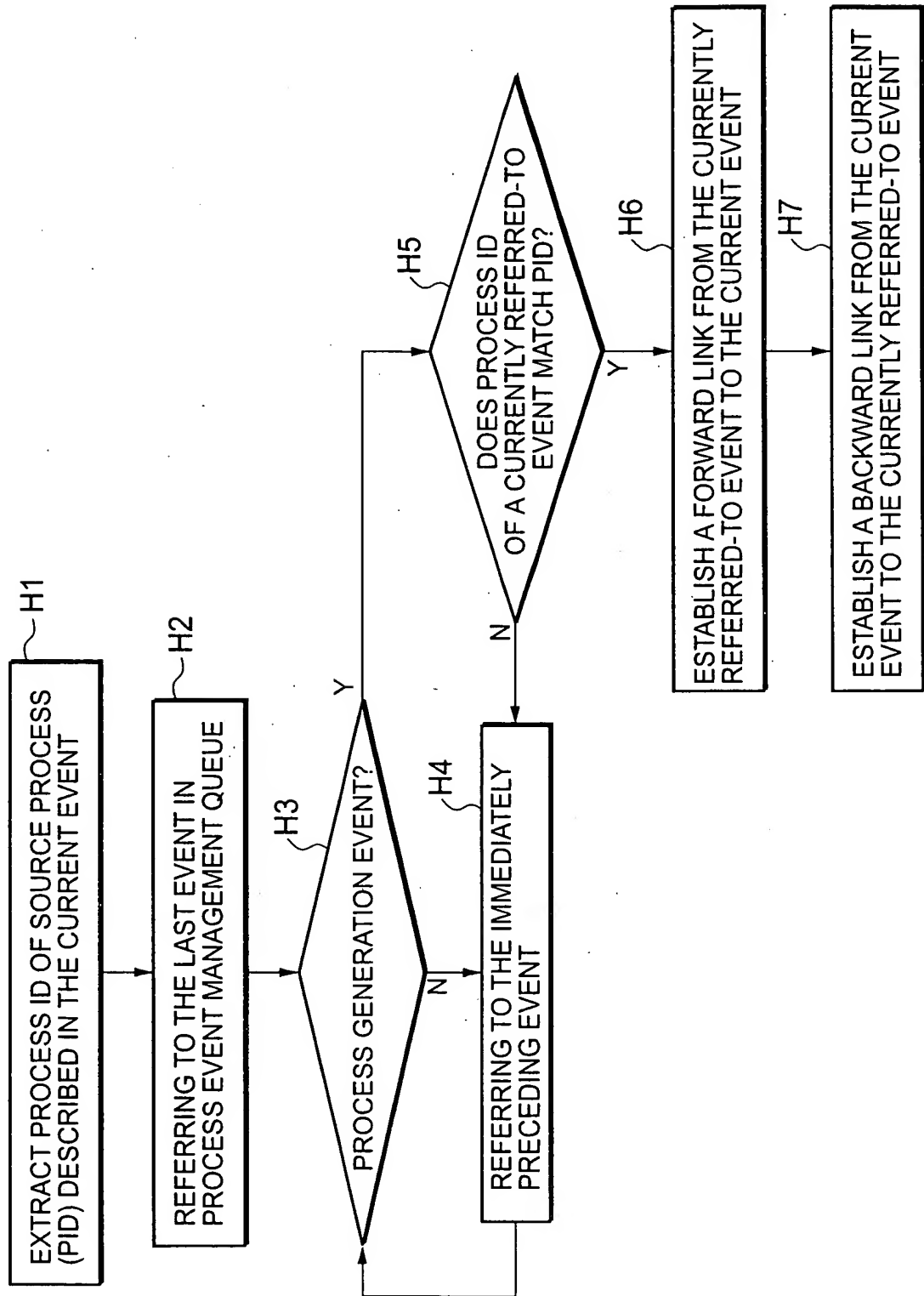
--	--	--	--	--	--	--

"FILE" EVENT MANAGEMENT QUEUE 

--	--	--	--	--	--	--

35/55

FIG. 37



36/55

FIG. 38

EVENT-CONTEXT COMBINATION = (E, B U F)



FIG. 39

4101 DT DEFINITION FILE

```

#(RULE 1) ALLOW WWW SERVER TO WRITE LOG.
0.0.0.0/0,<Inetinfo.exe>,FILE_WRITE,C:%winnt%system32\LogFiles%.*;ALLOW
#(RULE 2) ALLOW WWW SERVER TO READ CONTENT REGION
0.0.0.0/0,<Inetinfo.exe>,FILE_READ,C:%Inetpub%wwwroot%.*;ALLOW

#(RULE 3) ALLOW REGISTERED CGI THAT IS A SUBSYSTEM
OF WWW SERVER TO UPDATE DATABASE.
0.0.0.0/0,<Inetinfo.exe><regist.exe> $,FILE_WRITE,C:%data%client.db;ALLOW
#(RULE 4) ALLOW OUTPUT CGI THAT IS A SUBSYSTEM
OF WWW SERVER TO READ DATABASE.
0.0.0.0/0,<Inetinfo.exe><view.exe> $,FILE_READ,C:%data%client.db;ALLOW

#(RULE 5) ALLOW FTP SERVER TO WRITE ONTO CONTENT REGION
# BUT ONLY FROM MANAGEMENT DOMAIN 10.56.192.0/24.
10.56.192.0/24.^<ftpd.exe>+ $,FILE_WRITE,C:%Inetpub%wwwroot%.*;ALLOW

#(RULE 6) WWW SERVER DOES NOT WRITE TO FILE UNLESS
SPECIFICALLY ALLOWED
0.0.0.0/0,<inetinfo.exe>.FILE_WRITE,.*;DENY
#(RULE 7) INHIBIT ACCESS TO DATABASE REGION FROM
OTHER THAN ALLOWED PROGRAMS
0.0.0.0/0,.*,*.FILE_READ|FILE_WRITE,C:%data%.*;DENY
#(RULE 8) REWRITING OF CONTENT REGION BY OTHER THAN
ALLOWED PROGRAMS IS AN ATTACK
0.0.0.0/0,.*,*.FILE_WRITE,C:%Inetpub%wwwroot%.*;DENY

#(DEFAULT RULE) IF NO MATCH IS FOUND FOR ANY RULE,
THEN "ALLOWANCE"
DEFAULT;ALLOW

```

37/55

FIG. 40

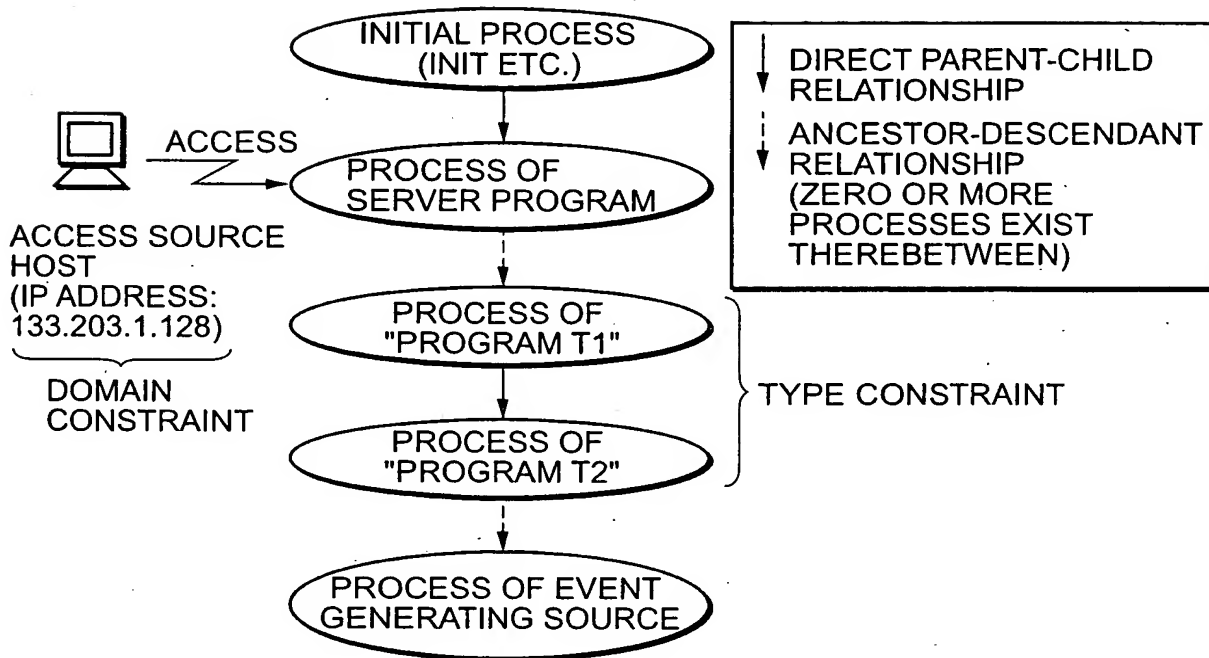
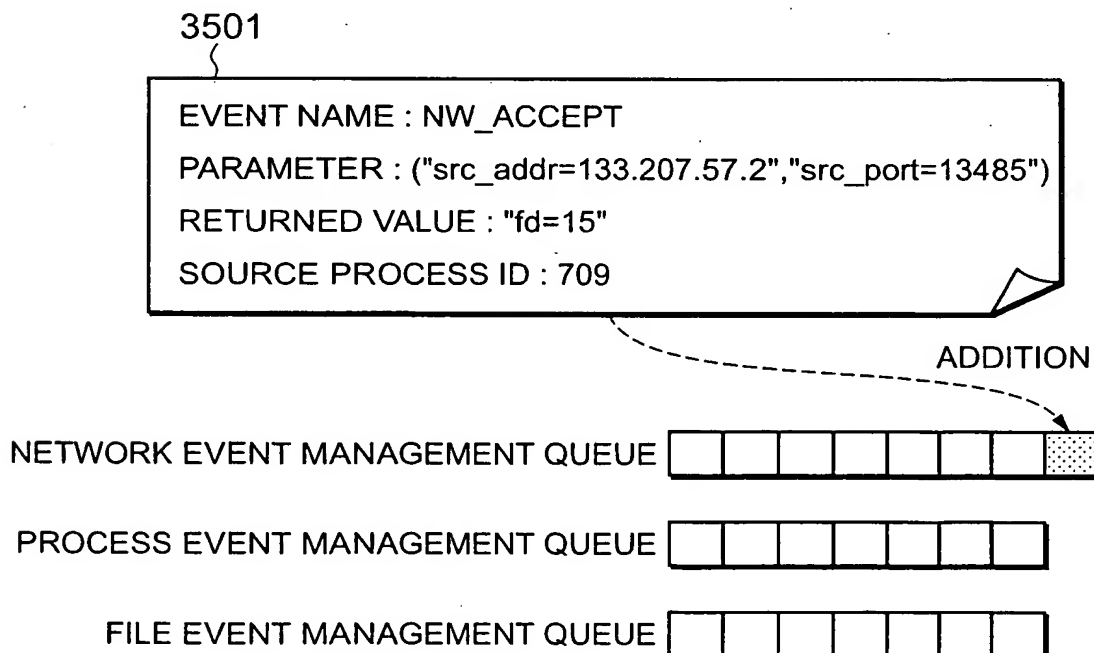


FIG. 41



38/55

FIG. 42

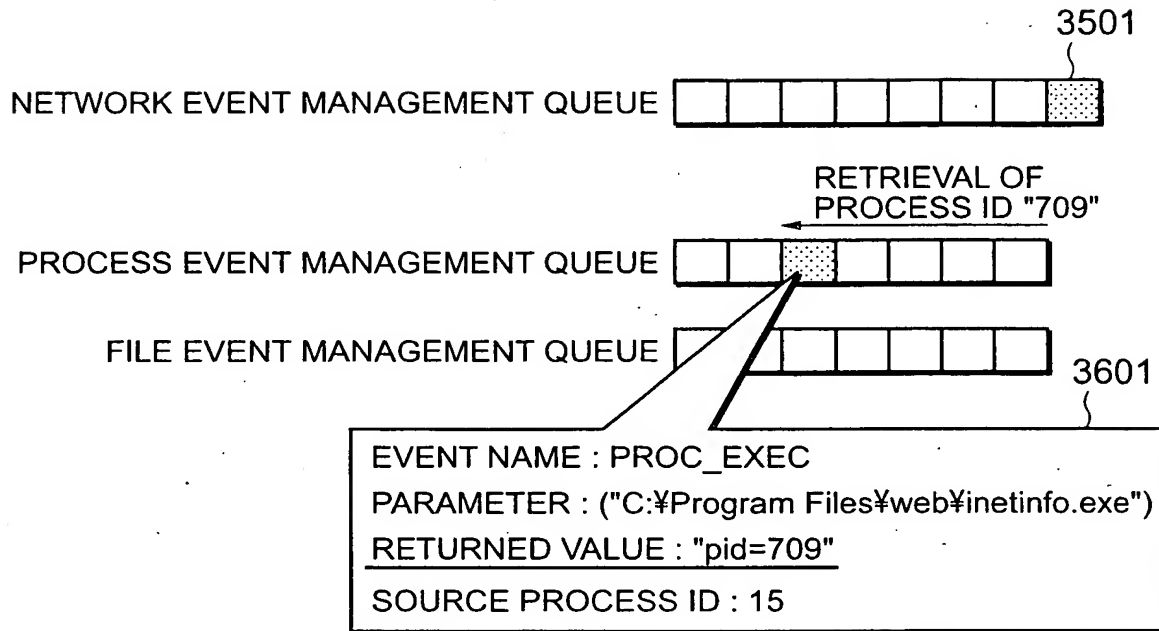
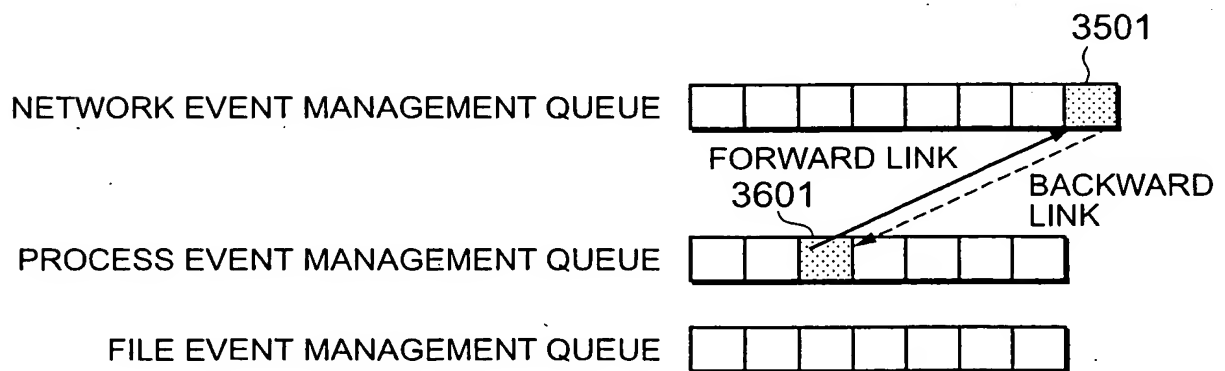


FIG. 43



39/55

FIG. 44

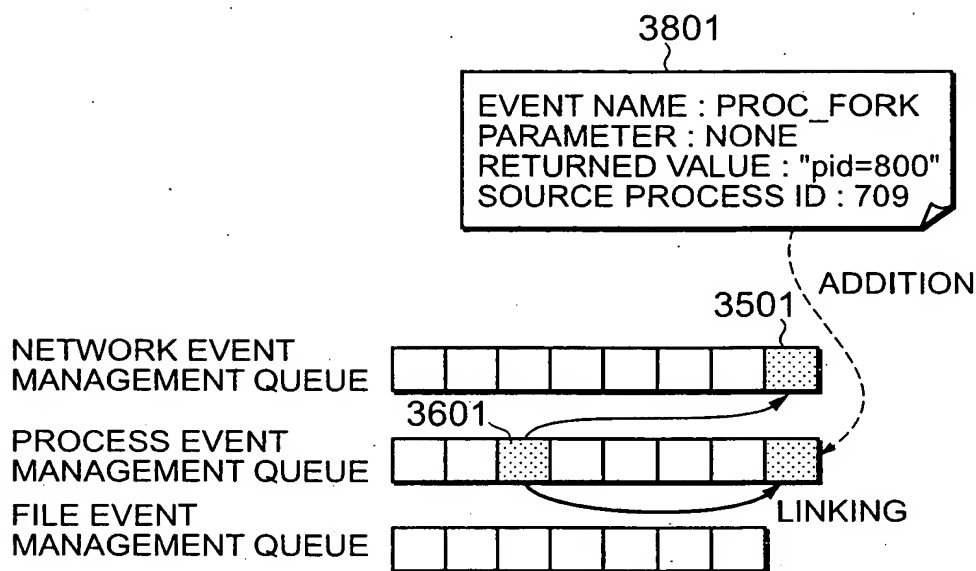
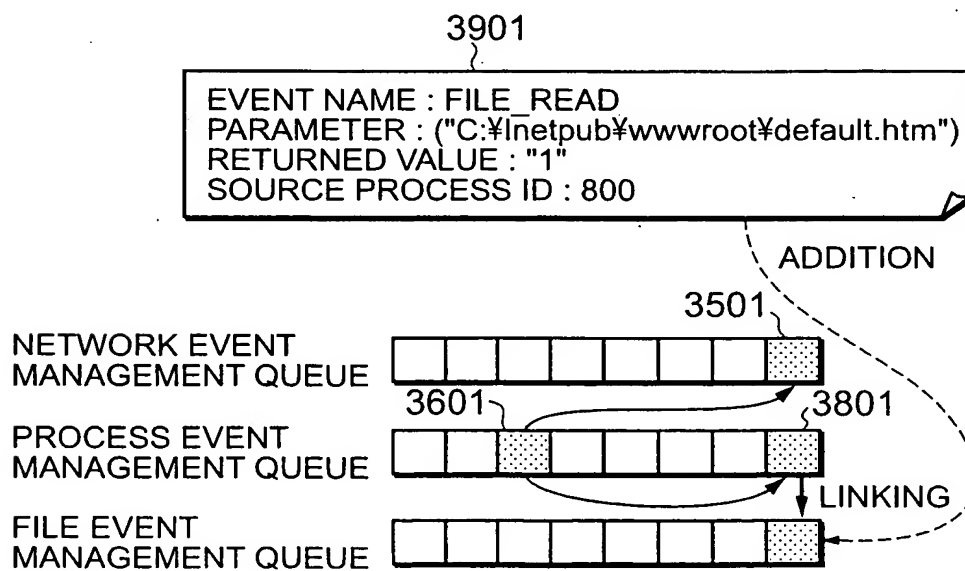


FIG. 45



40/55

FIG. 46

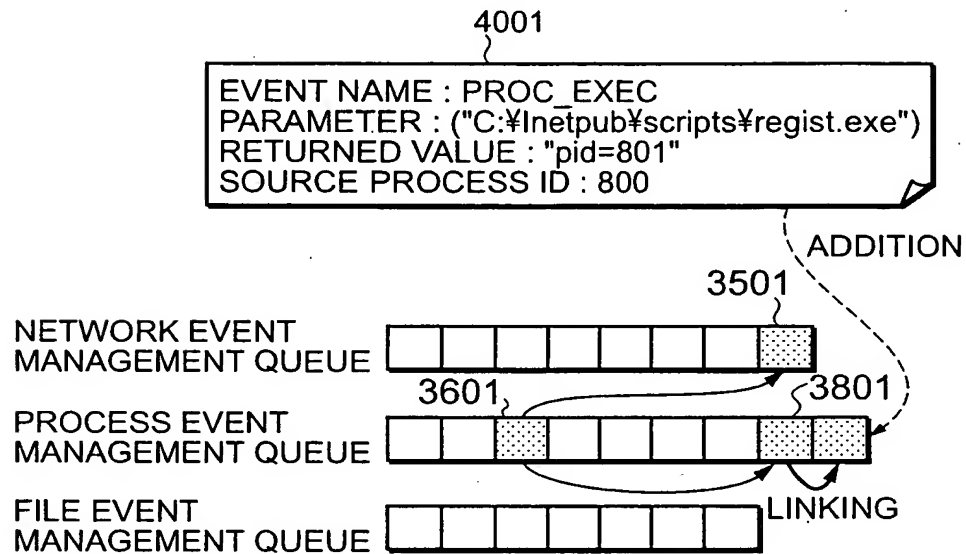
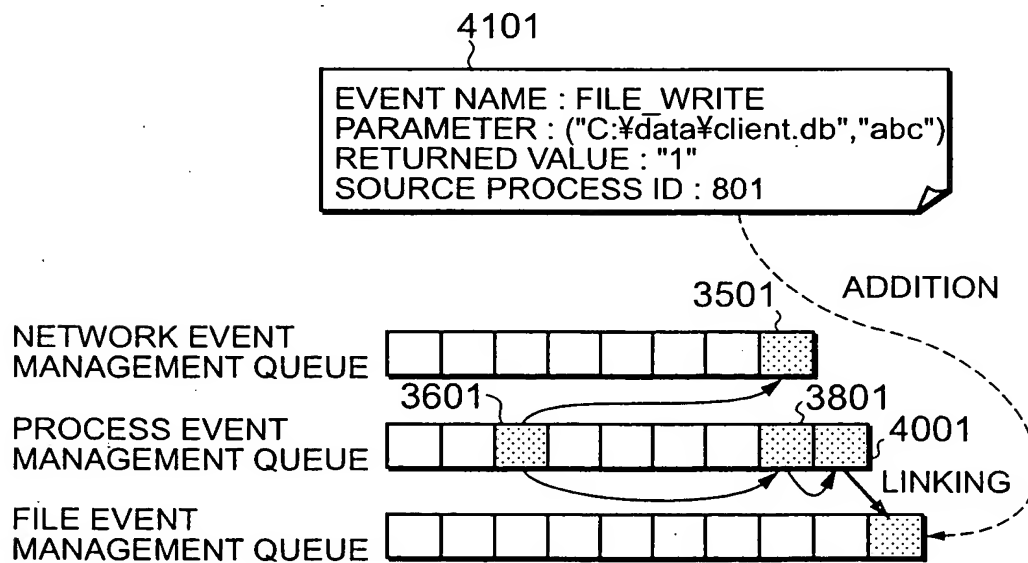


FIG. 47





41/55

FIG. 48

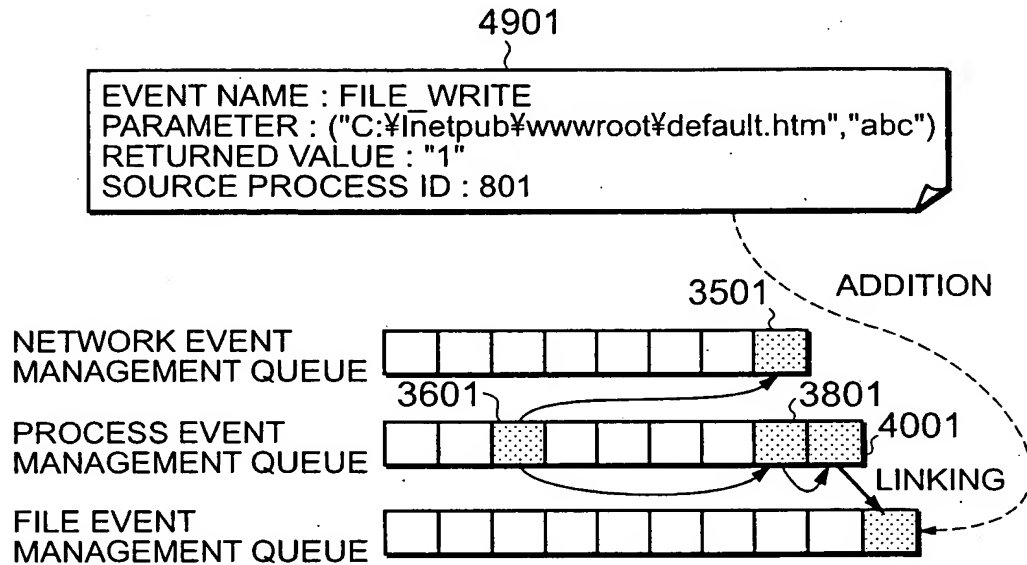
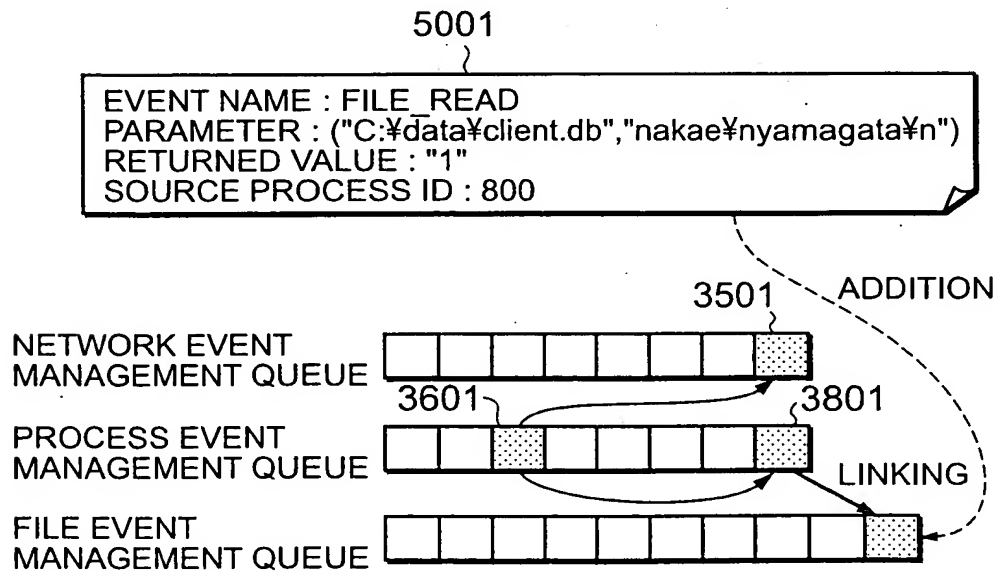
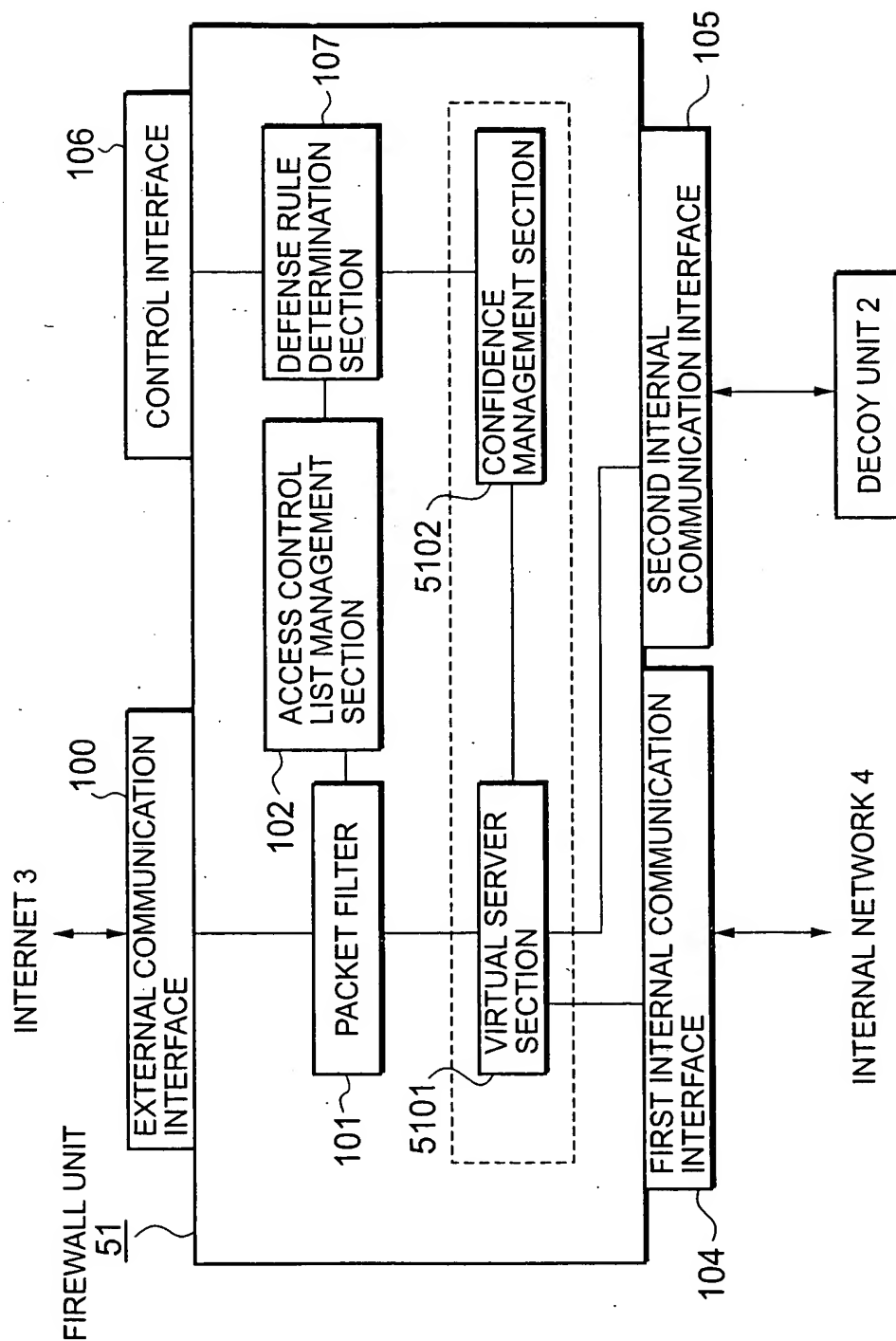


FIG. 49



42/55

FIG. 50



43/55

FIG. 51

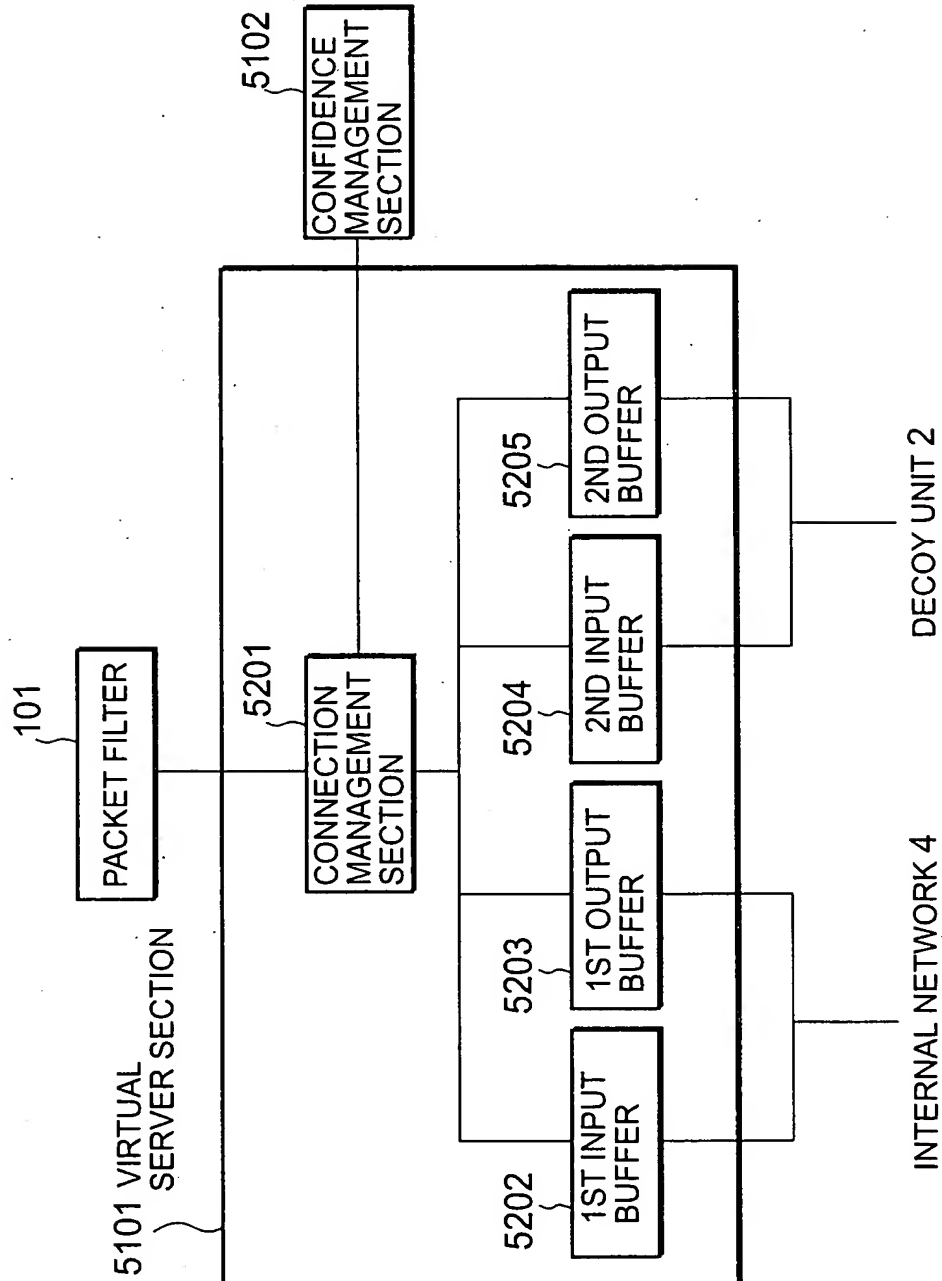
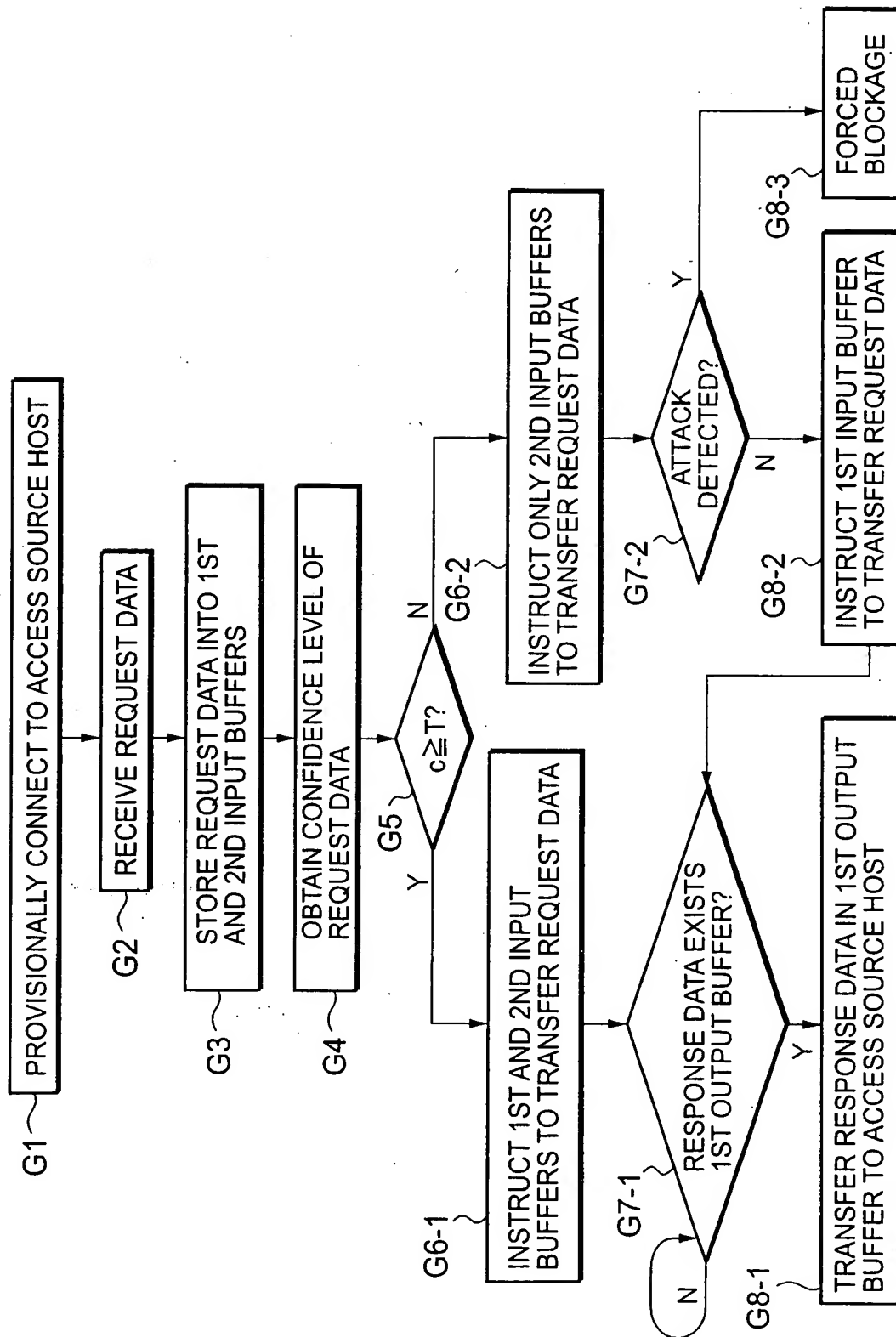


FIG. 52

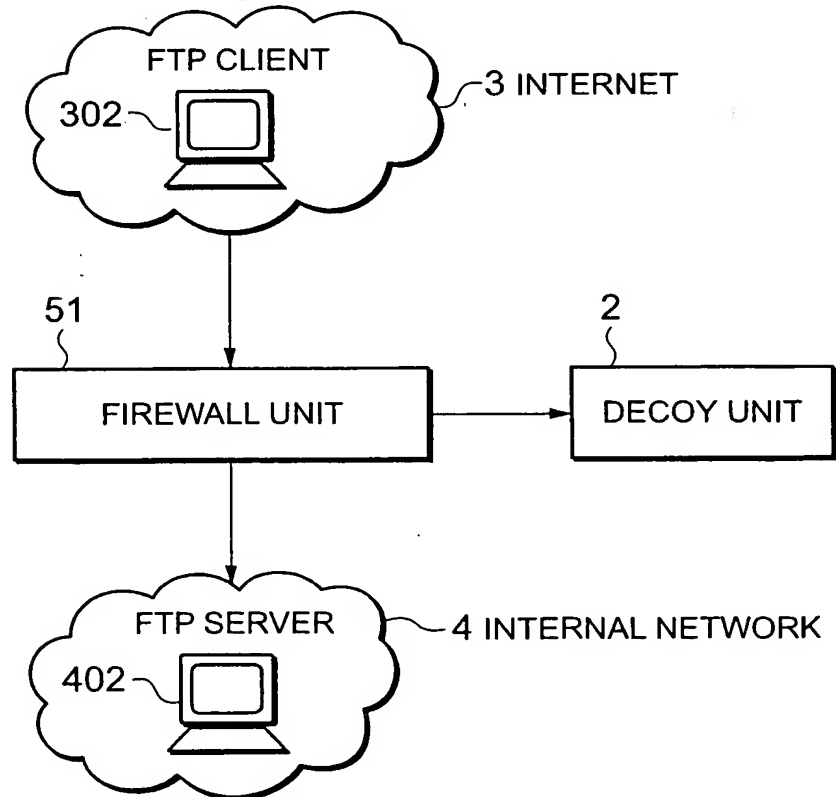


45/55

FIG. 53

REQUEST DATA	CONFIDENCE LEVEL
D0	1
D1	0
. . .	. . .
Dn	1

FIG. 54

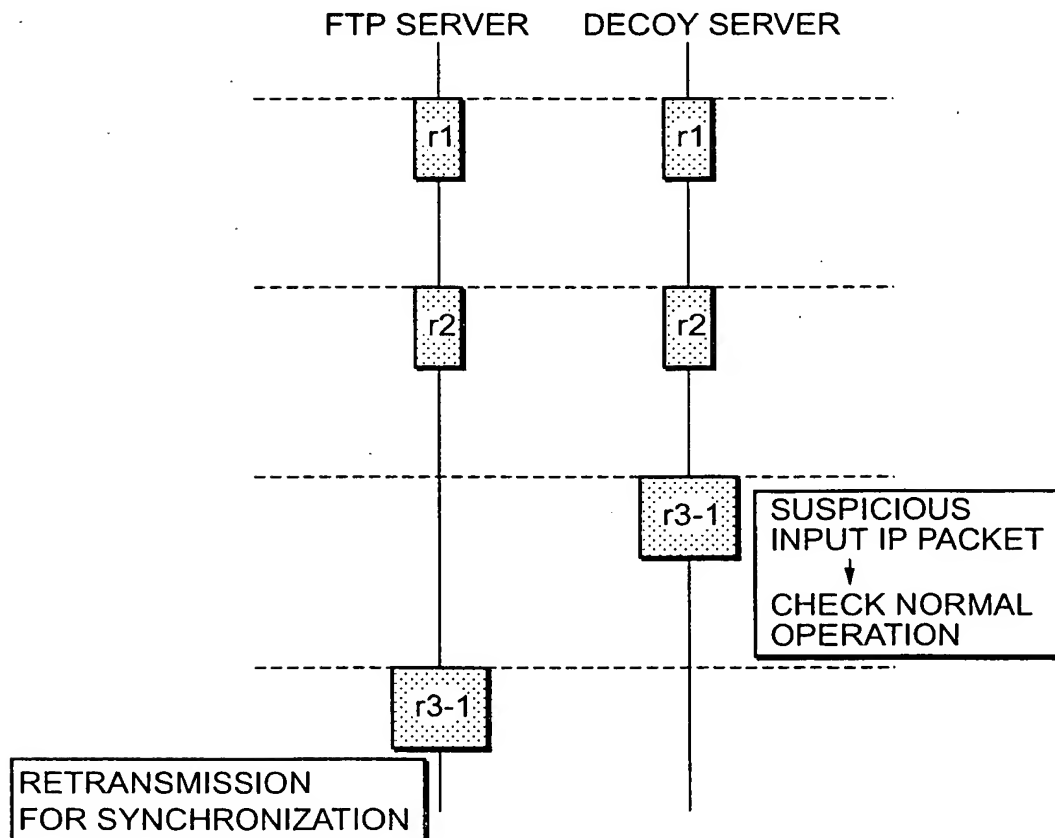


46/55

FIG. 55

REQUEST DATA	CONFIDENCE LEVEL
D0	1
D1	0
. . .	. . .
1	0

FIG. 56



47/55

FIG. 57

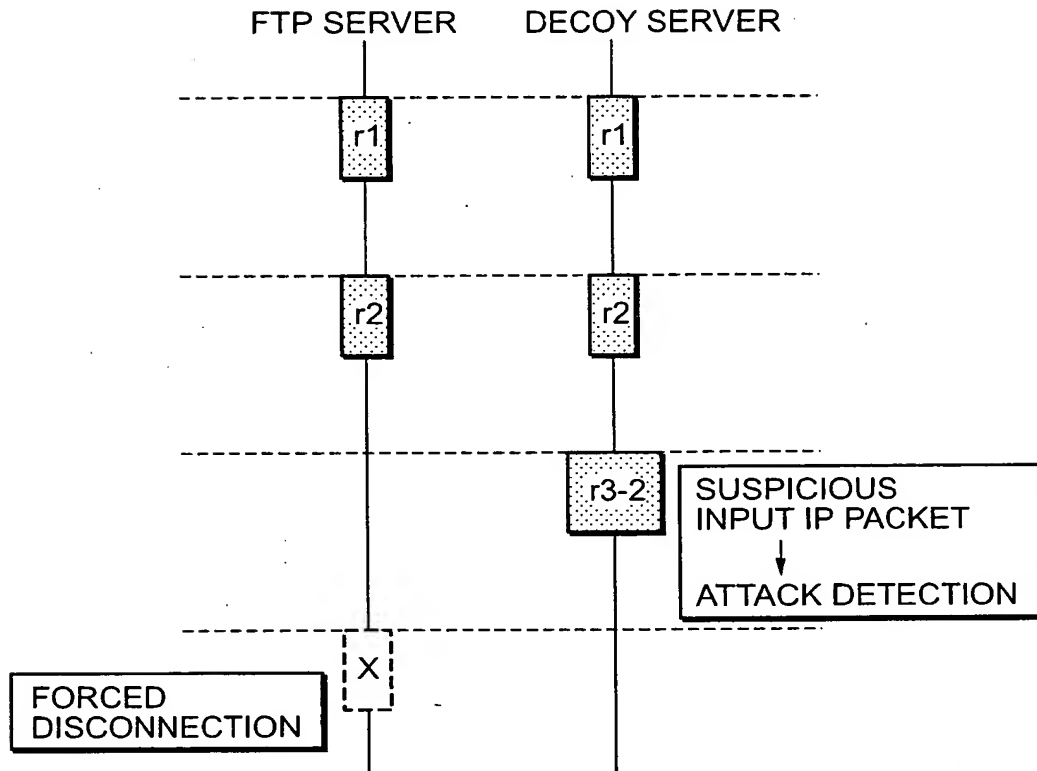
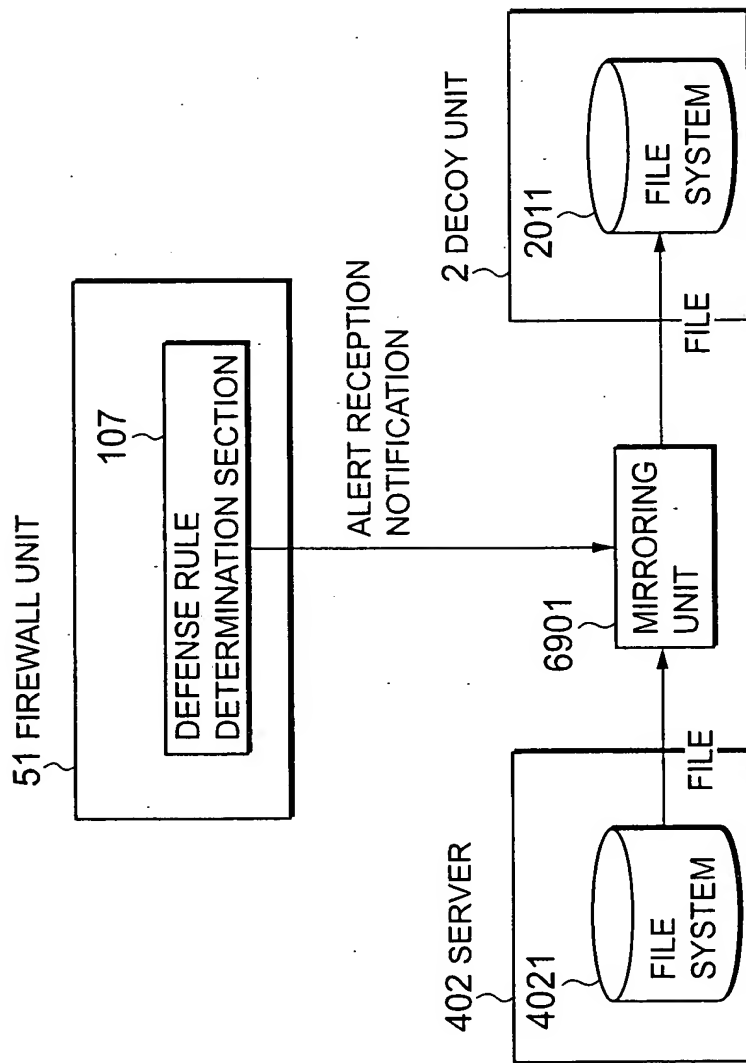


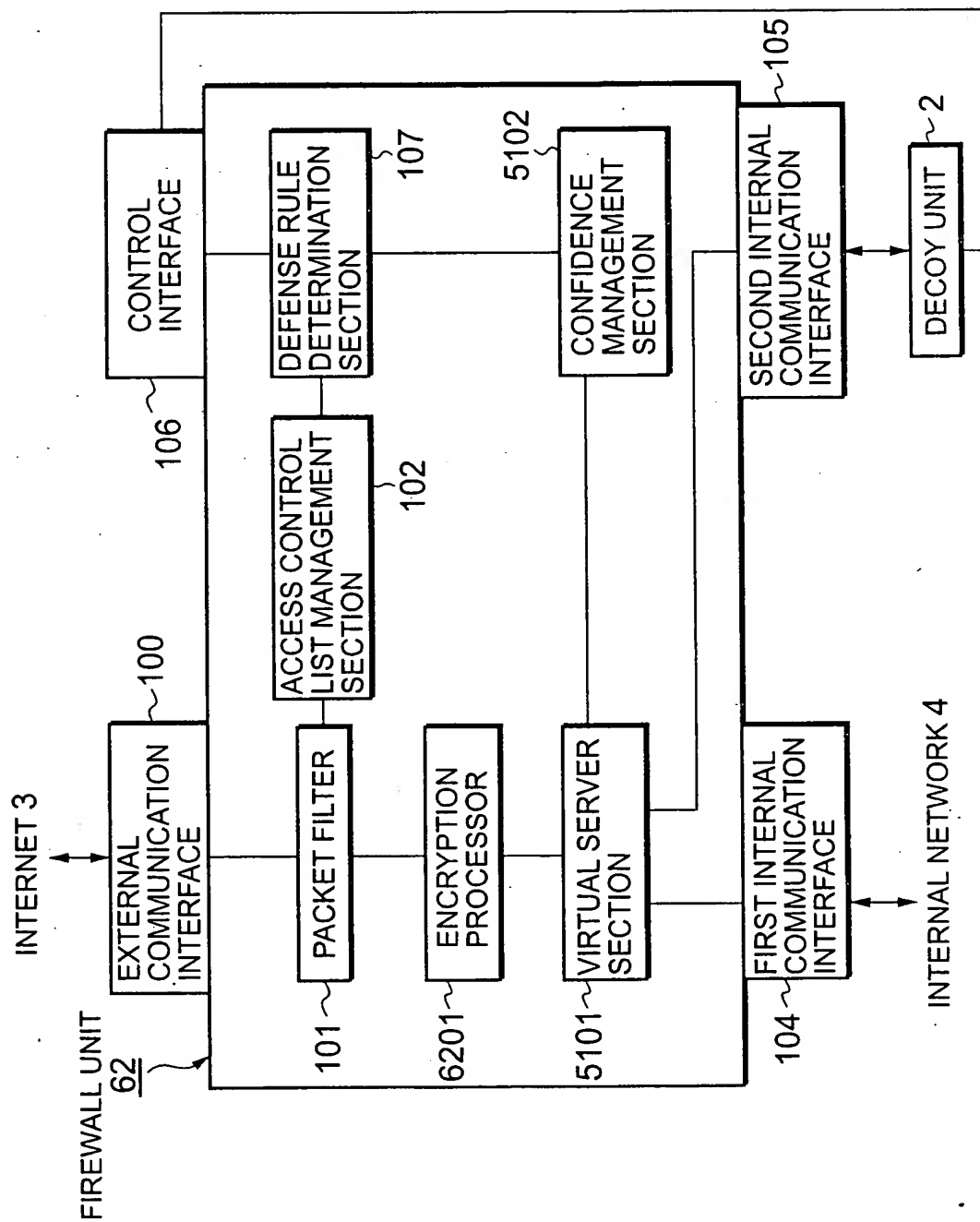
FIG. 58





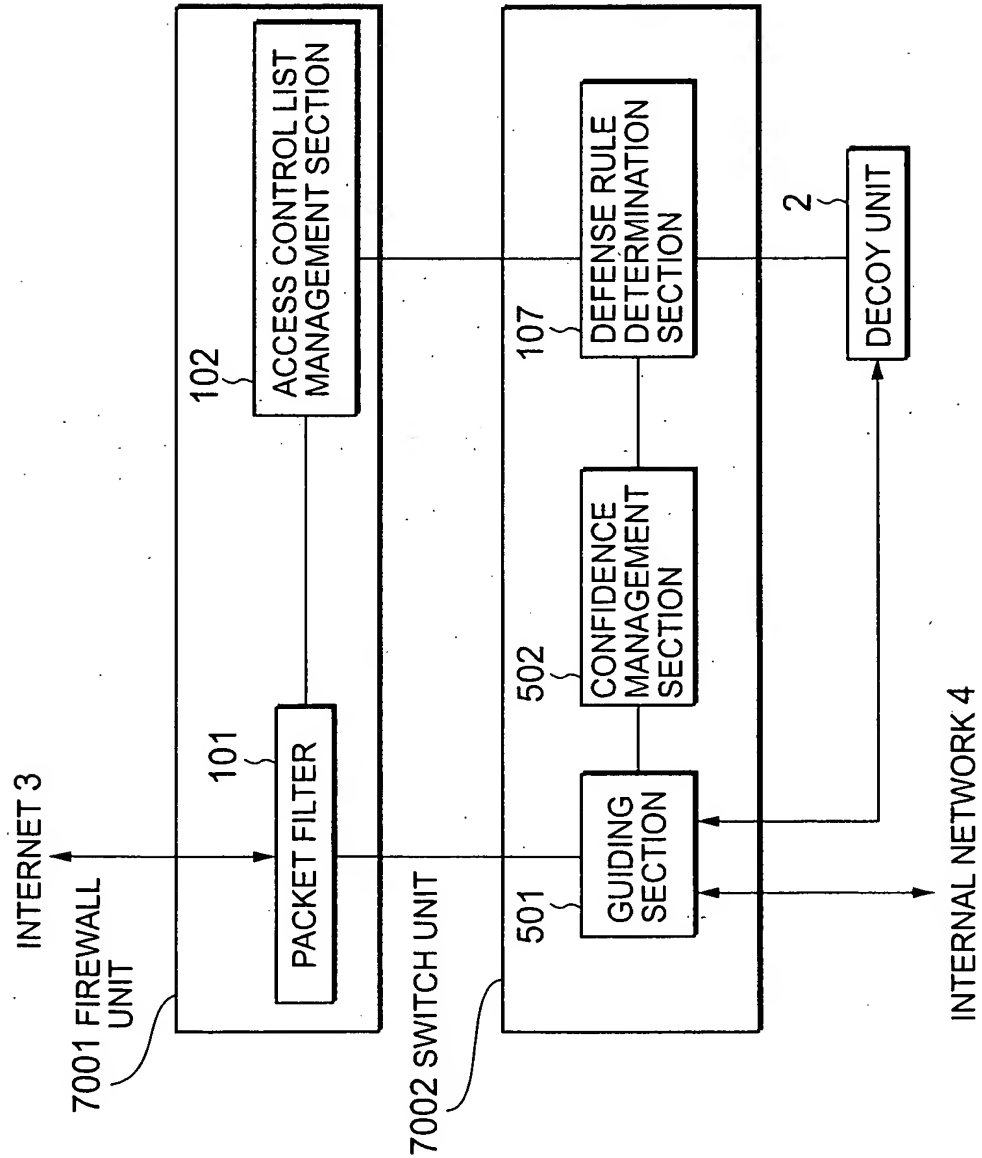
49/55

FIG. 59



50/55

FIG. 60



51/55

FIG. 61

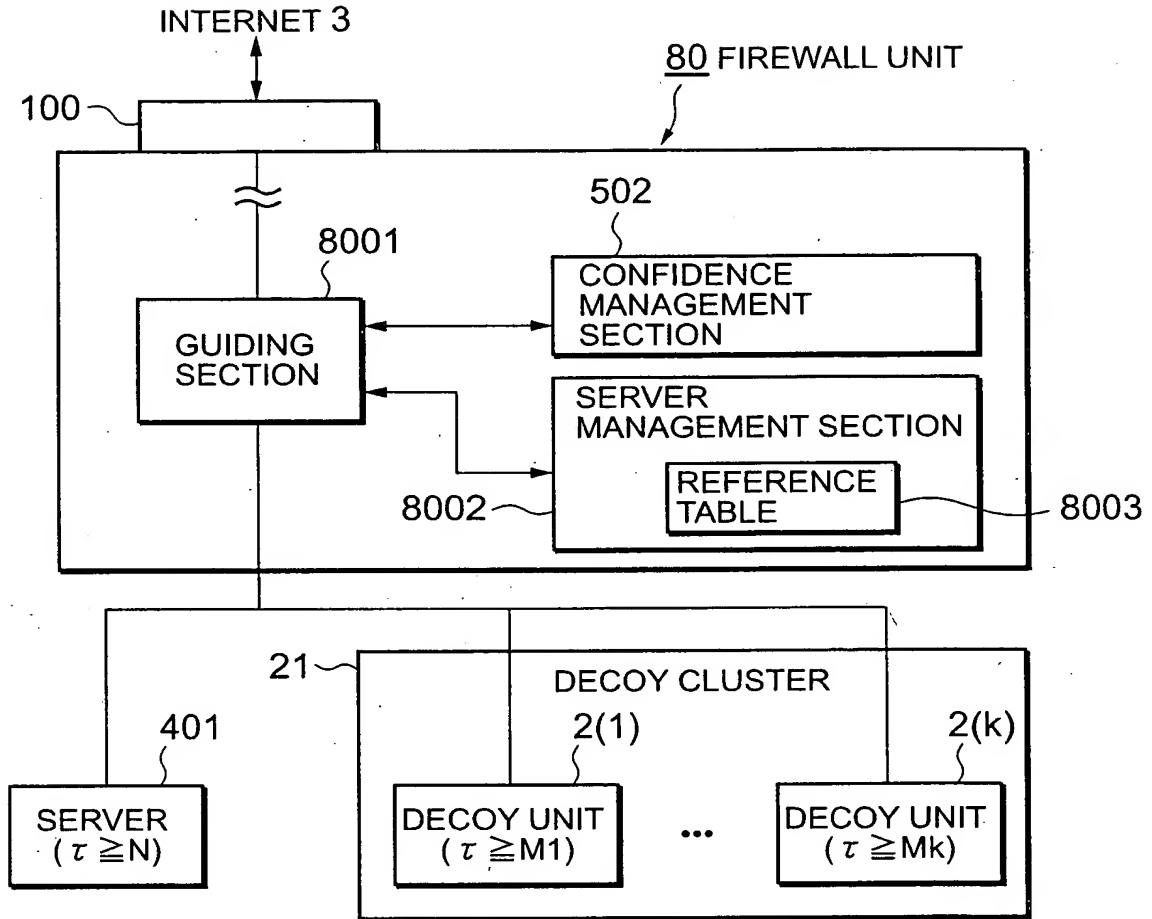


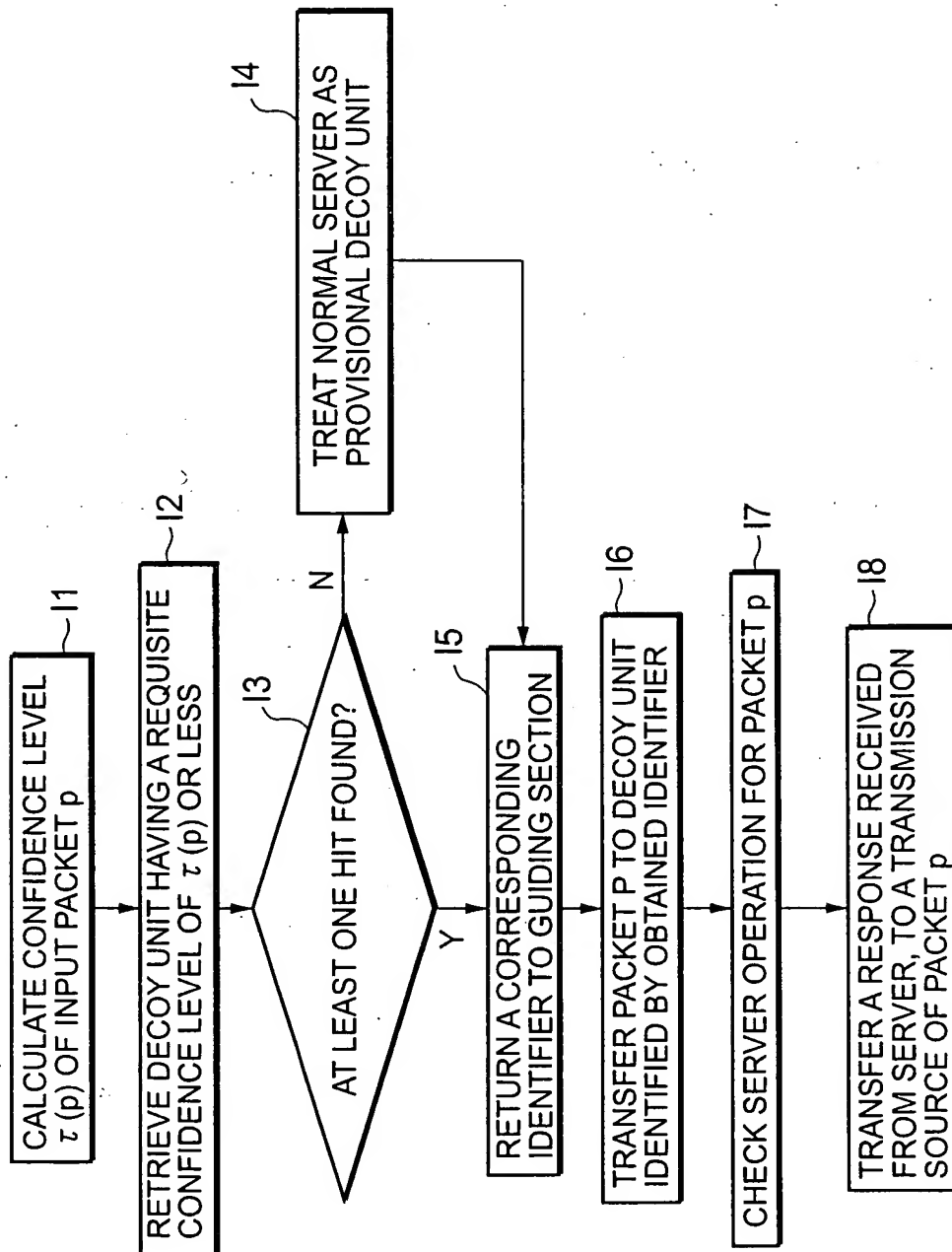
FIG. 62

8003 REFERENCE TABLE

SERVER IDENTIFIER	REQUISITE CONFIDENCE LEVEL
D1	M1
D2	M2
...	...
Dk	Mk

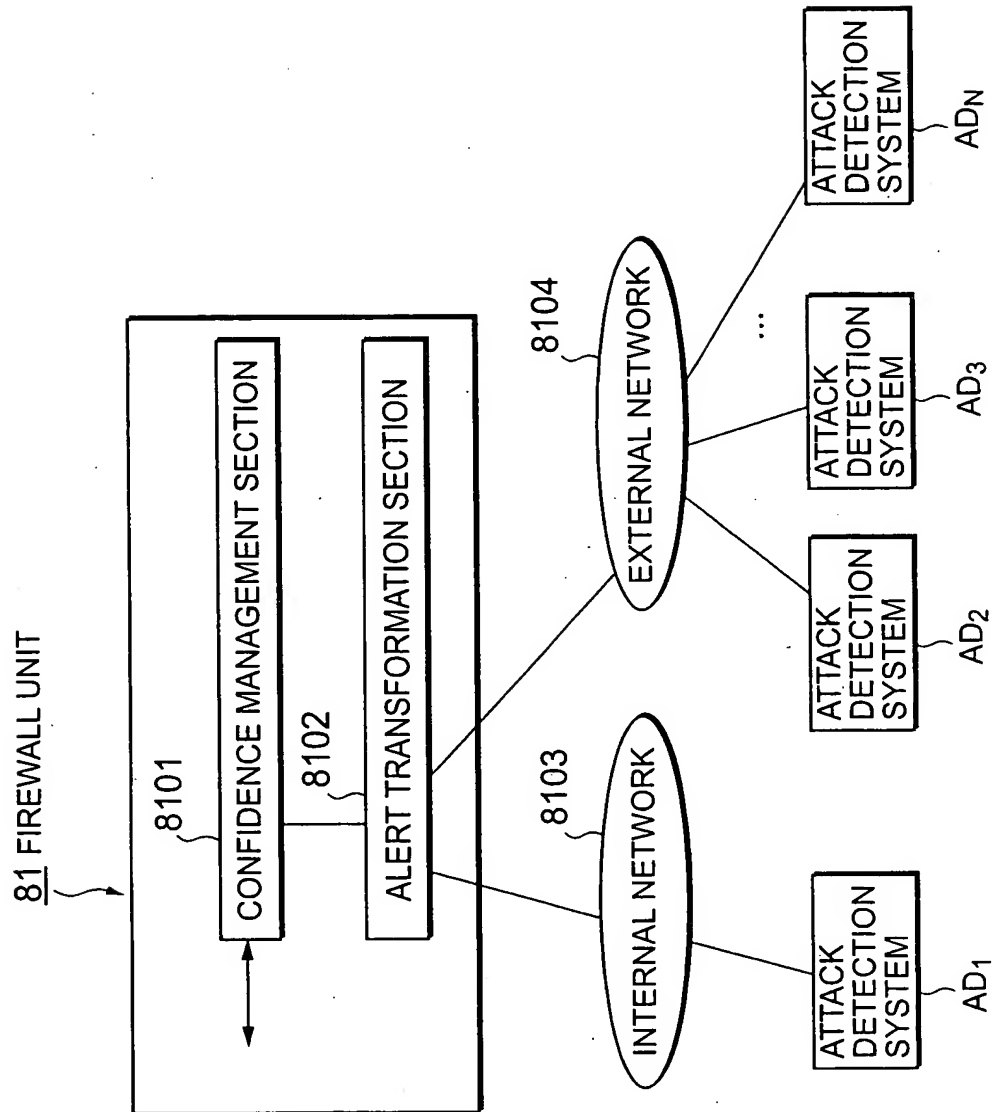
52/55

FIG. 63



53/55

FIG. 64



54/55

FIG. 65

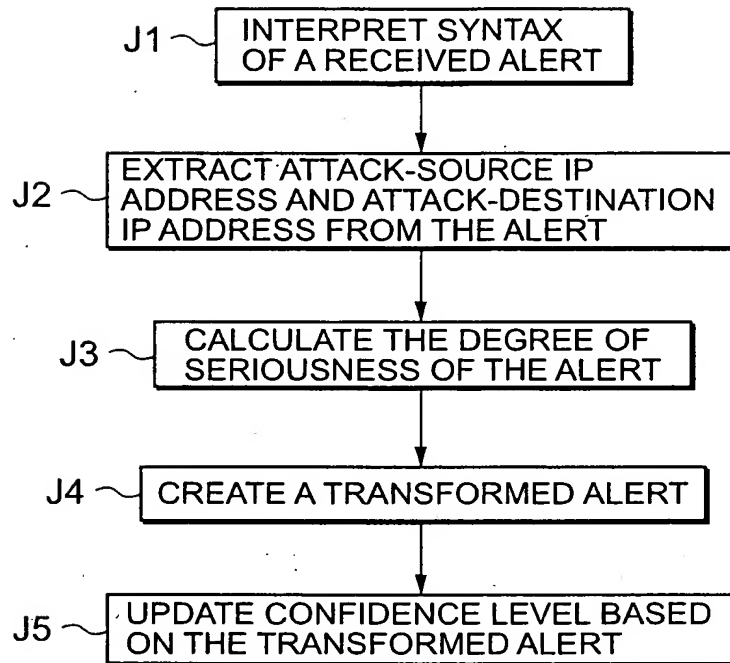
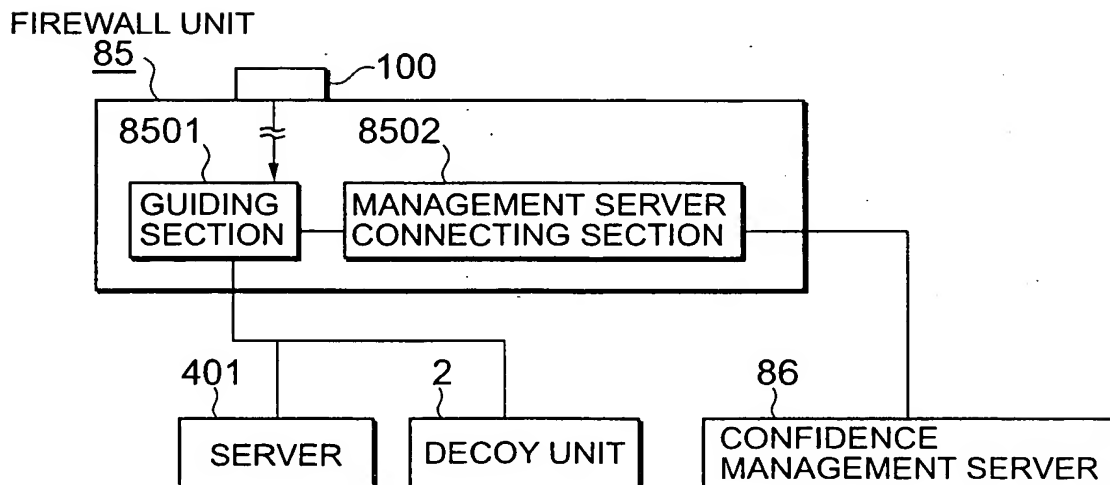


FIG. 66



55/55

FIG. 67

